Central IT-Infrastructure for serving several Central Checkout System Sets

Tim-Christin Hanschen[(1)], Jens Schmidt[(2)], Dr. Carsten Reese[(3)], Dr. Gilberto Arantes[(4)]

(1)
Universitätsallee 27-29
28359 Bremen
GERMANY
Email: Tim-Christian.Hanschen@ohb.de

(2)
Universitätsallee 27-29
28359 Bremen
GERMANY
Email: Jens.Schmidt@ohb.de

(3)
Universitätsallee 27-29
28359 Bremen
GERMANY
Email: Carsten.Reese@ohb.de

(4)
Universitätsallee 27-29
28359 Bremen
GERMANY
Email: Gilberto.Arantes@ohb.de

ABSTRACT

Most of todays OHB space missions are using a Central Checkout System (TERMA CCS or similar) for spacecraft testing throughout all AIT phases. Normally, a “Set” that means a checkout-system that consists to one spacecraft model, is isolated from the facility LAN. All services for running the environment have to be implemented for each set. A common set consists of one server, some clients and an infrastructure (storage, network, etc) that is adequate for testing. Usually, the infrastructure for each set is handled by the project itself.

The objective of this paper is to present a central infrastructure that can provide all needed network services, e.g. like Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) or Network Time Protocol (NTP) and common services like backup, version control system, and web services. Servers and clients will be provided as virtual machines. In the light of this central infrastructure, there would be a common IT-infrastructure for all projects. This will lead to harmonization and cross-functionalities that shall foster the process for usage, maintenance, and operations for any Central Checkout System deployed by OHB. This paper highlights the possible services, e.g. access the facility LAN for data-exchange or needed network-services, with the presented concept. The following features are covered in this paper:

- hardware-independent
- redundant
- scalable
- flexible
- reliable
- full-featured, all required services are implemented and could be used if needed
- virtual network, that means that the project networks are locally independent and could also be spread over external sites, e.g. Bremen, Munich, etc.
- services to the facility LAN could be granted on request
- reduced hardware costs

The whole infrastructure will be designed with a high level of redundancy, reliability, scalability and security independent of the used Central Checkout System. It can be used for any kind of Central Checkout System, for instance, TERMA CCS3, TERMA CCS5 or even the upcoming European common core, i.e. EGS_CC, is covered. It is also possible to provide different systems for each project. The projects will have their specific requirements and those shall be enveloped by the proposed the central IT-Infrastructure.

DESIGN

Traditionally in a CCS setup you have two subnets. One subnet is used for the CCS itself, that means for the server, the clients, a storage system and a printer. The second subnet is for the communication of the SCOEs. The CCS server and also the Test Conductor Workstation (TCWS) are connected to both networks. The CCS clients, printer and the storage are only connected to the CCS subnet.

A connection to the facility LAN is in the first step not designated but a connection will only be used for the CCS subnet.

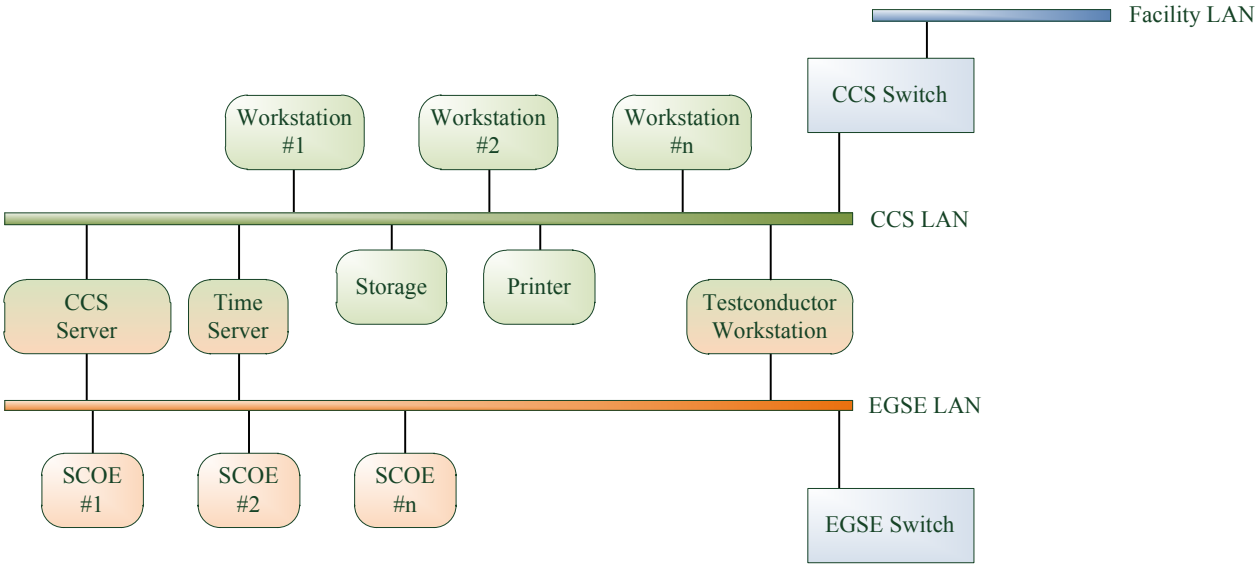

Fig. 1. Traditional CCS Setup

This traditional setup is very limiting in different ways. The first one is the connection to the facility LAN. At the beginning of a project the connection to the facility LAN always seems to be not necessary, but the need will increase abruptly when tasks with CCS starts. There must be a way to, at least, transfer files, e.g. scripts to the CCS and test results for analysis from CCS. There will also be nice-to-have features like using a central version control system or access to a central error reporting system for creating error reports in an easy way directly in the clean room.

The traditional design of an isolated EGSE setup will be weaken in the field of IT-infrastructure. The setups are no longer separated and isolated but connected in a central network-infrastructure. The separation will be done logically. It means that from physical side of view all setups are connected somehow, but from project view access is restricted to only needed connections and services. The advantage is that it will be possible to use services for all projects, e.g. time services or DNS (domain name service). Needed network services can be granted or revoked in an easy and flexible way.

If the network is available for all projects the next step will be a centralization of the server-infrastructure in order to achieve a better utilization of resources. Server-infrastructure means servers itself, but also storage and backup devices. Physical servers or NAS devices are no longer needed for the project setups. The central infrastructure will also provide the ability for running virtual machines. In this case, the CCS servers run on central physical servers and can be accessed from project side. Data will be stored on central storage subsystems. That means that every project that is part of the central IT-infrastructure can access storage automatically. Backup is part of the central infrastructure so everything that is stored on the central storage subsystem is automatically backed-up regularly. The project does not have to take care of

those services, e.g. storage. The virtualization of the servers will also bring much more flexibility because there is no need for the projects to buy and maintain server hardware. It is only necessary to request resources (additional servers) which will be provided in the virtual infrastructure.

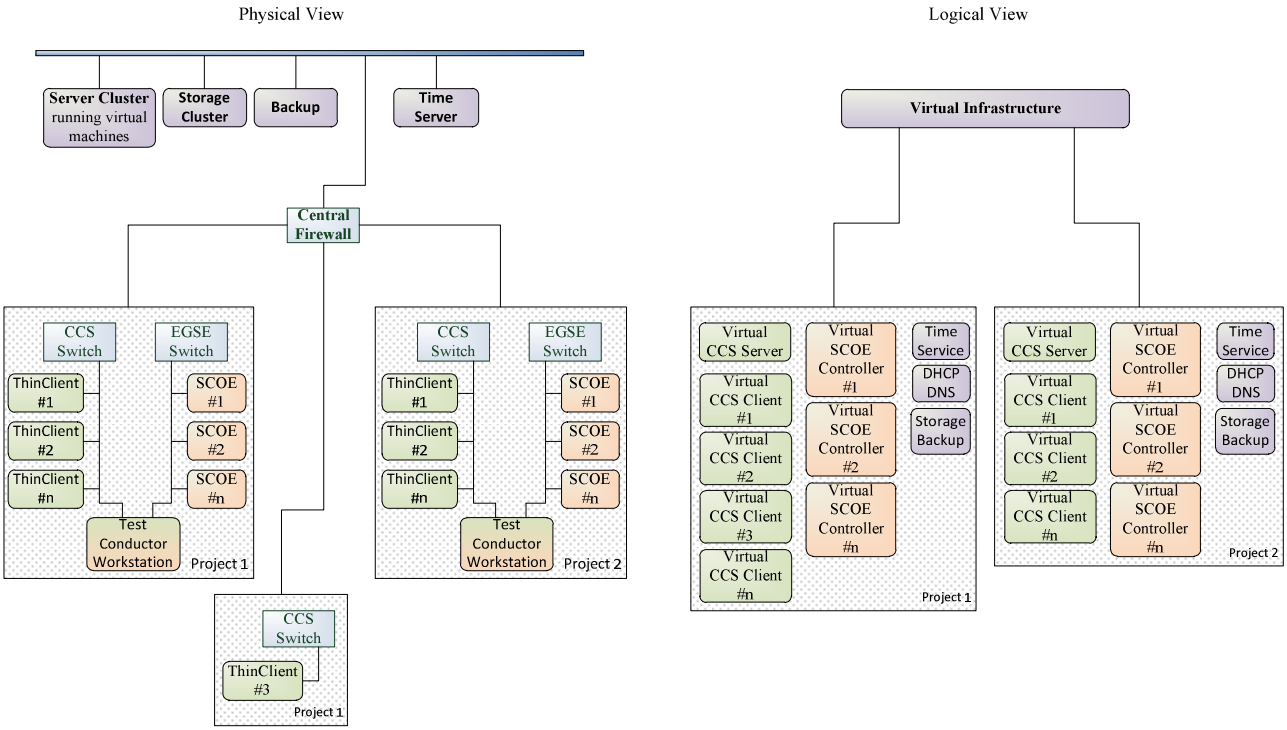

Fig. 2. Central IT-Infrastructure

Virtualization

A normal PC installation have to be done in this way:

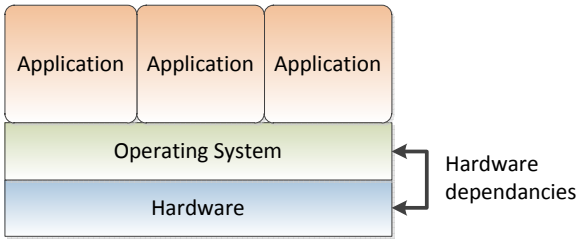

Fig. 3. Physical Server

An operating system has to be installed directly on the hardware. The operating system have to take care that all hardware devices can be used. In this case, it is necessary to have a device driver installed. On top of the operating system there will be the applications, e.g. CCS.

Virtualization means that the operating system is no longer installed directly on a PC or server. There will be a hypervisor installed on a server, which is a software that is able to create a virtual PC, that means that CPU, memory, hard drive and interfaces are only build in software. One physical server is able to run several virtual machines (VM). The VM itself does not depend on hardware any longer, because in the VM there are only virtual devices under usage. That means, practically, there is no need to reconfigure the system if the physical server changes.

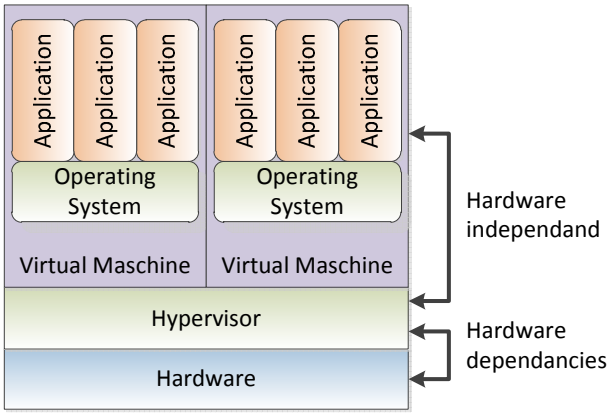

Fig. 4. Virtual Server

With a virtual server and client infrastructure there are several advantages. The installed systems do not depend on hardware any longer. The systems will be provided as virtual machines, the device drivers i.e. are only necessary for virtual devices and not for real hardware. Thus, in case of a massive hardware failure the VM could be run on any hardware that runs the hypervisor. Another advantage is the increase of redundancy. There is the possibility to cluster two or more physical servers in a cluster. The VMs that are running in the cluster will automatically be moved from one physical server to another if there is a hardware failure or if the utilization of a server is too high and demanding. From VM point of view there is no interruption. The movement of the VM is done in the background. It is also possible to create copies of VMs in order to get a test system. Moreover, desktop virtualization reduces administration tasks, i.e. if you use desktop virtualization you can define groups of desktop images. Within a group you can create a master image. If someone wants to use a virtual desktop the system will create an image out of the master image. If there is the need for a software update or for additional configurations it is only necessary to change the master images consequently all other system will be updated automatically. The virtual desktop runs on the hypervisor, so communication to the CCS server is much faster, because the communication is within the cluster.

Advantages at a glance:

- better utilisation of hardware
- more flexibility
- hardware independency
- redundancy
- reduced hardware costs

NETWORK

Global Structure

Because there is a connection between the facility LAN and all project LANs it is mandatory to protect the networks against each other. This is done via a central firewall with protects the project networks against the facility LAN. On the other hand, it protects the projects against each other. All network traffic is routed via the firewall. Access rules in the firewall will control the flow of data and allow or reject network services and connections. Each project will be represented by a virtual local network (VLAN) that means that the network will be defined logically over different network devices. The advantage is that a VLAN can be spread over the whole network infrastructure. The project network will become independent from the location. Another advantage is that VLANs are isolated and protected against each other. From network point of view all services are pre-configured and usable and can be applied to the project on request in an easy and flexible way.

Project-Networks

The project network is comparable with the traditional CCS-setup. There will also be a CCS LAN and an EGSE LAN. The connection of the SCOEs and test equipment will be maintained. The standard PCs that are used as CCS clients will be replaced by thin clients, which are actually simple PCs with no local storage. These clients will only be used to connect to a virtual CCS client installation that runs on the central server cluster. The client itself is more or less only used as an terminal. The interconnection between CCS server and CCS client will only be established directly in the server cluster.

External Sites

During a project lifecycle there will always be the situation that external sites have to be visited for test or launch campaigns. These external sites will be connected to the facility LAN via an encrypted VPN connection. From project network point of view there is no difference whether the CCS setup is located physically at the facility LAN or connected via an encrypted VPN connection from then launch site. The services which are granted on the facility LAN will also be available at the external site. Connection to a server at the facility site or remote access can be granted easily.

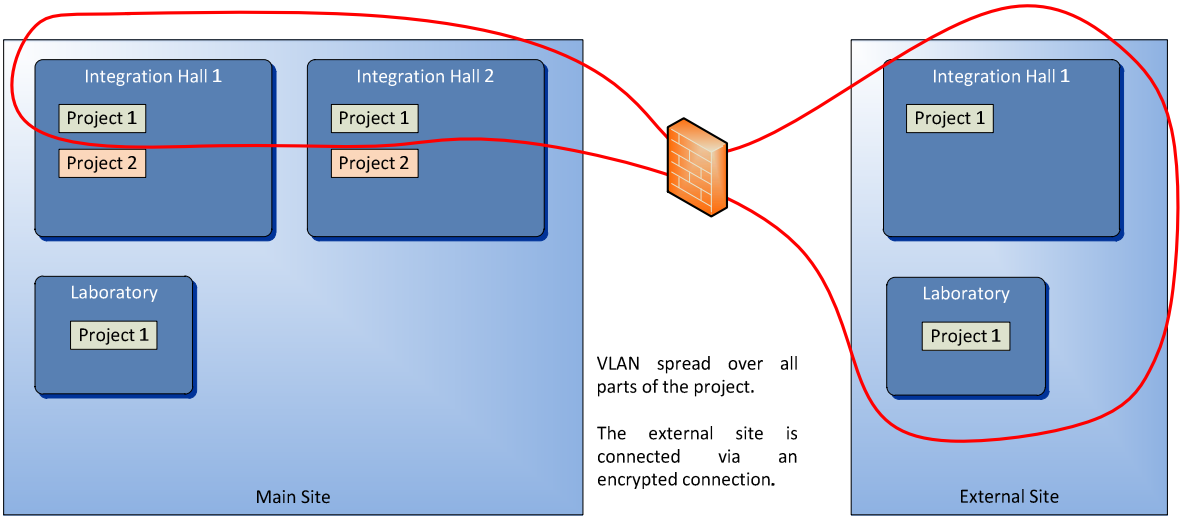

Fig. 5. VLAN and external connection

From project point of view there is no difference where you connect to the network. You will have access to all resources independent of the location.

NETWORK-SERVICES

DHCP and DNS

In order to achieve an easy manageable network it is mandatory to use DHCP and DNS.

DNS is a service that is used to create references between an IP address of a device and a hostname so that devices can be reached via their hostname. Data packets that are sent through the network only reference an IP address. For better readability it is a good idea to use hostnames instead. The DNS service will resolve a hostname to the appropriate IP address.

Hostname	IP
Prj1_Client01	*192.168.1.10*
Pjr1_Client02	*192.168.1.11*
Prj2_Client01	*192.168.2.10*
Pjr2_Client02	*192.168.2.11*

In general there are two ways of distributing IP addresses in a network. The first one is to distribute IP addresses manually, which may lead to errors because of the distribution of double addresses by mistake. The second way is the use of DHCP. Here the distribution of address is done automatically. Each device will get an address maybe out of a special address range or depending on the media access control address (MAC). The DHCP service will be the central point of address distribution. Both services will be available for all projects from a central point.

Time Services

In a CCS setup all devices that means CCS server, clients and also SCOEs should use a common time reference in order to sync communication in the setup. A good reference could be the PTB in Braunschweig, which is an atomic time reference that is very accurate but can only be reached via internet. Because a CCS setup is generally not connected to the internet network time servers e.g. from Mainberg or TimeTools are used. These devices are quite expensive and traditionally needed twice for each setup. In a central IT-infrastructure it will be possible to use the PTB as the first reference and one network time server as a redundant, internet-independent device. The reference time will be forwarded to each CCS server which will be the reference for the corresponding CCS setup.

File Services

In every project there will be sooner or later the need for file services. There is no chance, in an isolated setup, to transfer data to or get data from a CCS setup, except the use of external storage devices for exchange. Transfer to the CCS setup e.g. for putting scripts on the system. Transfer from the CCS setup in order to get session result for analysis. The use of external storage devices, like USB sticks, is always dangerous in terms of viruses.

With the central IT-infrastructure in place it will be possible to have a access to a central file server. Data that is copied to the file server is automatically checked against viruses so the danger of getting infected will go down. Because of a connection between the project networks and the facility network it will be possible to create exchange folders for each project so that data can be accessed directly from a personal workplace. Access rights can be granted based on personal user accounts in the facility network corresponding to the rights for the projects.

Remote Desktop

There may be the need for a Remote Desktop (RDP) to a CCS setup. This would be used for controlling a running session, performing an administrative task like software update and also for debugging reasons. Because of the central firewall that protects the projects against each other and also protects the projects against the facility LAN it is also possible to grant or reject remote access. It is possible to allow RDP for a special user or for a special workstation. The access can be restricted to a special CCS client in then setup or to the whole project subnet.

Version Control System

A version control system like Subversion (SVN) is necessary to manage scripts and libraries for a CCS. Each file that is check-in is stored in a repository with a special version so that changes are transparent and reversible if they are faulty.

Traditionally, each CCS setup uses a dedicated SVN server. In order to harmonize and centralize services it is possible, due to a central IT infrastructure, to use one central SVN server that can be used from all CCS setups. Each project will get an own repository on the central SVN server. For the projects there is no need to think about backups or failover because this will already be implemented. Because of the centralization it will also be possible to share a repository for different setups within one project. The idea behind is that there are files, especially libraries, that can be shared between several models, because they are equal for all set. With a central version control system you can divide between common files and specific files which make it much easier to keep all files in sync.

CCS-SETUP

Server

Traditionally each CCS-setup will make use of an own dedicated server. The server will serve all CCS clients for just one dedicated setup. A failover system is mostly not planned.

The requirements for CPU and memory of a CCS server are not very high. In order to utilize the hardware in a much better way and get failover capabilities the CCS servers are virtualized. Therefore, the servers are provided virtually on a server cluster. Two or more physical servers are connected to a cluster and are able to run 20 or more virtual machines (VM). The characteristics of a virtual machine, e.g. memory, CPUs or network interfaces are defined logically. The VMs do not depend directly on the hardware layer any more. On top of a very flexible and reliable environment the cluster also provides a failover capability for all VMs.

Clients

CCS clients are only used to connect to a running CCS session that runs in the CCS server. On a client there are no database or power applications running. The only demanding application will be synoptics that are graphical user-interfaces.

There are two possibilities. The first one is to keep “fat clients” as workstations. From administration point of view all clients have to be installed and configured like usual PCs. From users point of view these clients are performing quite well. The second possibility is the use of “thin clients”. Thin clients are only used as an interface to the user that means they only connect remotely to a virtual machine that runs on the server. From administration point of view it is very easy, because there is only very limited administration effort necessary. It is not necessary to install CCS software on the clients because this software will run on the virtual machine. Software updates for the virtual machines can be done on a server in a “master template” that will automatically be distributed to all clients. From users point of view the performance may be worse. Costly, the hardware price of a thin client and fat client are comparable.

MONITORING

The central IT-infrastructure will also provide a central monitoring. In general, we separate between a monitoring for IT related devices like servers, PCs, network equipment and a monitoring for test equipment like SCOE controller, special devices or tasks that are necessary to AIT and EGSE.

Each project will have an own monitoring console with project related detailed information on. The global EGSE department will also have a console that will give an overall view for all projects and the whole infrastructure.

The monitoring system is not only a passive view on the infrastructure, but also an active alerting system. If there are problems, e.g. a filesystem is full or an important task is not running, the system will automatically send a notification to the responsible persons.

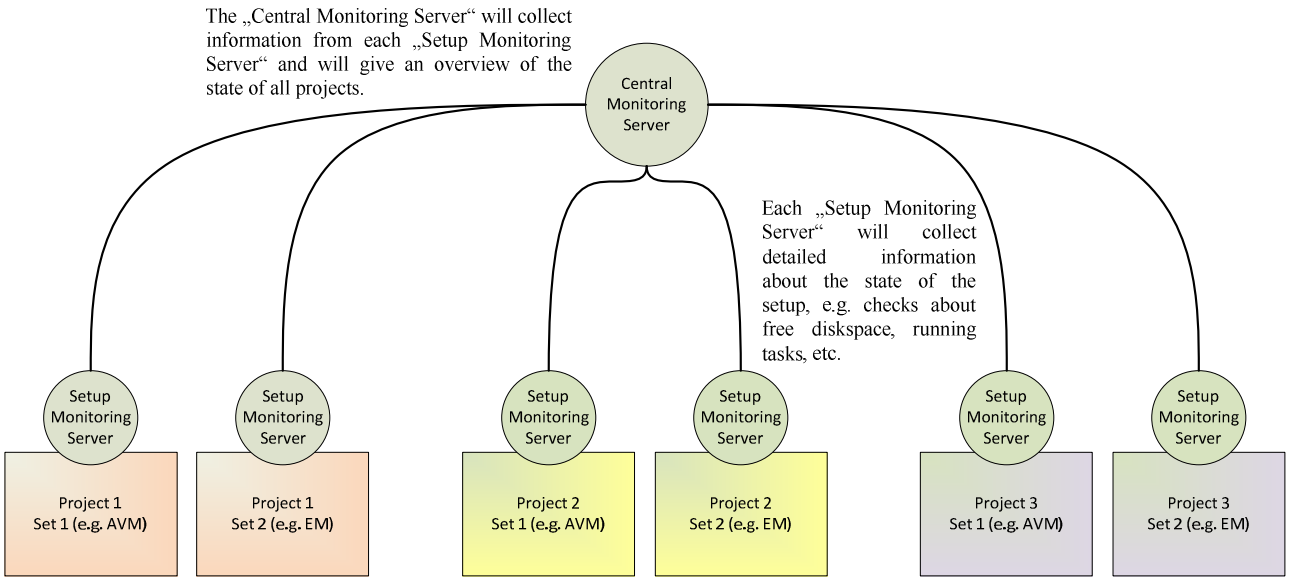

Fig. 6. Central Monitoring Structure

IT-Infrastructure

For the IT-infrastructure the monitoring will cover “standard” parameters that will show how healthy the IT-infrastructure is:

- utilization of CPUs
- level of filesystems
- accessibility of servers, storage systems, switches
- accuracy of time-services

EGSE

For the EGSE there are also standard IT related parameters that have to be monitored, especially for most of the SCOE controllers, that are usually normal PCs. Additional monitoring is necessary for devices like signal generators, modems and other electronical devices. The monitoring should also cover tasks or services on the devices that are mandatory to run.

CONCLUSION

If the traditional way of setting up a CCS environment, that means an environment of separated and isolated project networks, will be turned off, there are a lot of improvements in security, robustness, features and also decreased costs. This will be a further step into modern and seminal way to handle projects.

REFERENCES

[1] VMware vSphere ESXi and vCenter Server 6.0 Documentation
[2] Documentation Resources for VMware Horizon 7 version 7.0
[3] Citrix XenApp and XenDesktop Documentation
[4] Citrix XenDesktop Reference Architectures
[5] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
[6] BSI-Standard 100-2: IT_Grundschutz-Vorgehensweise
[7] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
[8] BSI-Standard 100-4: Notfallmanagement