Superior Flexibility for the Control Room Workplace

Thomas Singer[1], Ursula Kretschel[2] and Michael Schmidhuber[3]
German Space Operations Center, DLR Oberpfaffenhofen, Germany

The workplaces typically found in control rooms for spacecraft operations are rather plain and old-fashioned. This results in many limitations. Workplaces nowadays consist of one or more PC-type computers with one or multiple monitors attached to it. These usually have a locally installed operating system. The system is configured for one type of task in one dedicated project. Flexibility, cross-operability and redundancy are limited. They are usually provided by restricting the users into identical setups - a lowest common denominator. Free computing resource allocation is additionally restrained by separation of networks due to network security aspects. From the user-side it is however desirable to allow a user to choose from a variety of setups, regarding the allocation and arrangement of computing resources to monitors, the easy access to redundant resources and the parallel use of resources. The ultimate desire is the elimination of the physical assignment of resources like keyboard and mouse to specific computers and monitors. The goal is to have flexible workplaces that allow rapid reconfiguration of control rooms for temporary use, training and simulation areas as well as multi-mission operations with heterogeneous systems resulting in vastly higher efficiency in control room usage with reduced administrational efforts. Based on virtualization techniques a framework has been developed that allows secure access to server-hosted desktops. It ensures existing security policies while giving access to all control center resources. This paper demonstrates first results of the approach taken by GSOC for implementation in an evaluation environment and the plans for implementation in control rooms in the near future.

I. Introduction

TRADITIONALLY, the setup for control rooms is based on well-established techniques and the application of technical innovations is typically avoided except for such cases where special features are needed. This leads to very stable and reliable systems which of course is very beneficial for operations. However, these conventional systems have a significant disadvantage. Their flexibility is highly limited due to several existing dependencies like the strict assignment of the O/S to certain hardware. Therefore, reorganization for another satellite mission is very complicated and time-consuming.
At GSOC, investigations have been carried out concerning the question of how modern IT solutions could be used in order to establish much more flexible systems in the control rooms. As a result, it will be possible to support an increasing number of concurrent missions in the future.

II. Current Situation in the Control Rooms

The workplaces typically found in control rooms for spacecraft operations are rather plain and old-fashioned. This results in many limitations.

Workplaces nowadays consist of one or more PC-type computers with one or multiple monitors attached to it. The computers usually have a locally installed operating system. The whole system is configured for one type of task in one dedicated project leading to limited flexibility, cross-operability and redundancy (Fig. 1).

[1] 82230 Wessling, Germany; thomas.singer@dlr.de
[2] 82230 Wessling, Germany; ursula.kretschel@dlr.de
[3] 82230 Wessling, Germany; michael.schmidhuber@dlr.de

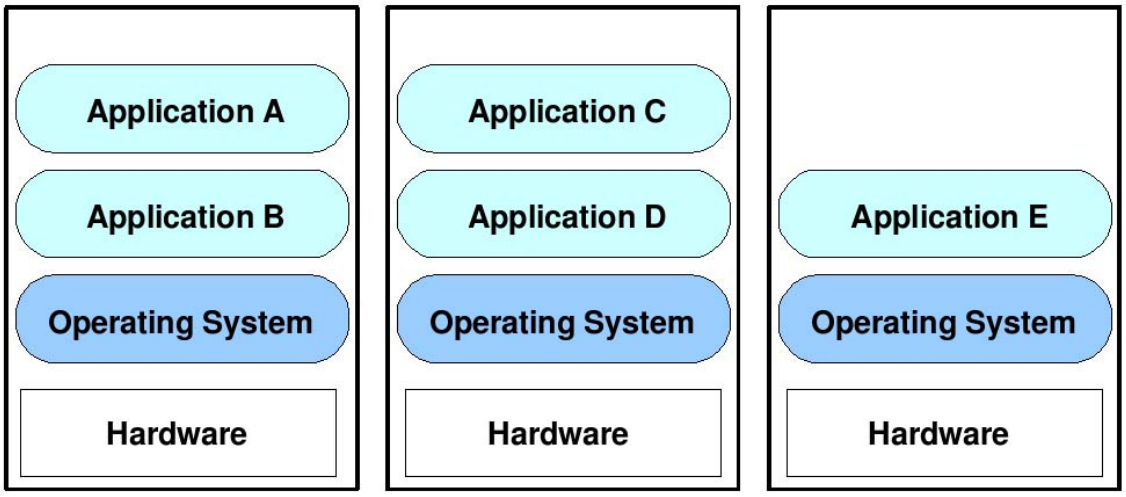

Figure 1. Current control room setup. Each workstation with locally installed O/S is used for one well-defined type of task.

Using the control room for another purpose like testing, simulations, emergency support or even for another project, will in most cases lead to different requirements concerning the applications, software versions or even the O/Ses installed on the workplaces. Resulting from this, an enormous amount of time and administrative work is needed to reconfigure the entire control room - and within this period the control room cannot be used at all.

Free computing resource allocation is additionally restrained by separation of networks due to network security aspects.

III. Which Improvements can be made?

By using modern IT solutions in the control rooms, there will be advantages for both operators and administrators. Furthermore the hardware can be reduced which should result in savings. The main objective is the possibility of using control rooms in a much more flexible way than in the current setup. This is especially important because of the increasing number of satellite projects at the GSOC MultiMission Control Center. For optimal support of all projects the existing control rooms may not be reserved for certain projects for a longer period of time in the future any more. Ideally each control room can be used for all satellite missions involving only minimal reconfiguration effort. This also means that the operators will be able to switch quickly and easily between different setups like training, simulations, etc. using just a single client device. In addition, applications running in external networks can be accessed from the same client device in a secure way. Besides the above mentioned there will be also significant advantages for administrators. On the one hand, the number of installations can be reduced because of the lower number of hardware needed in the control rooms. On the other hand, the maintenance for each system will be simplified which should lead to shorter downtimes.

IV. Technical Approach

A.More Flexibility by Implementation of Abstraction Layers

In a first step, it is necessary to decouple a specialized desktop environment from a dedicated workstation. This is not a new idea, as solutions like Windows Terminal Services have been providing a stable platform for centralized computing for several years. The applications installed on the server can be accessed by any client device able to contact the server over the network. Modern workstations usually support multiple monitors, so that it is also possible to display two or more desktops hosted on server platforms (even with different O/Ses) on only one client device installed in the control room. This shows how the hardware can be reduced in comparison to the traditional control room setup, where two or more workstations were needed for the same purpose. With this step being accomplished, nor a user is dependent on a certain workstation, neither a project is on a certain control room.

Although the above mentioned step eases the restrictions for operators in the control room, the resulting setup is

still very inflexible from an administrative point of view. At this stage, the fixed assignment of an O/S with the installed applications to certain hardware has only been moved from the control room to the server room. In order to loosen this, a virtualization layer, also known as hypervisor, is implemented. This hypervisor is installed directly on the server hardware and provides an environment for running VMs on top of it. The virtual hardware presented to the VMs does not match the real hardware, but consists of standard components. Because of this, it is even possible to still run old O/Ses in VMs that could not be installed on a new server hardware directly any more. In principle, a VM can simply be cloned or moved to a virtualization layer installed on another server hardware by just copying all of its files to a datastore accessible by that hypervisor. For this task, the VM has to be powered off and is therefore not available while copying it.

In order to gain more flexibility, especially concerning hardware failures and maintenances, it is necessary to abstract a VM from the hypervisor on a dedicated server. This can be accomplished by building a pool of identical servers with hypervisors which all have access to a centralized storage system where the files of the VM reside. In this way, every single server of the pool is capable of running the virtual machine on its own resources like CPU and RAM. In case of a hardware maintenance, the running VM can be migrated to another server of the same pool without any impact to the end users. The files of the VM which include the O/S, the installed applications and all data always remain on the storage system.

The next logical step is to break further dependencies. This can be achieved by encapsulating applications from the underlying operating system in a way which is transparent for the user. For this purpose, another abstraction layer is inserted which is called application virtualization layer. Basically, there are two approaches for virtualizing applications. The first option uses portable applications. These can be created from conventional applications with so-called portable application creators. The result is a self-contained executable file which includes everything required to run. Thus it is possible to run even such programs that could not be installed on the underlying O/S in the normal way (e.g. older programs on modern O/Ses or vice versa). Figure 2 shows the flexibility resulting from this.

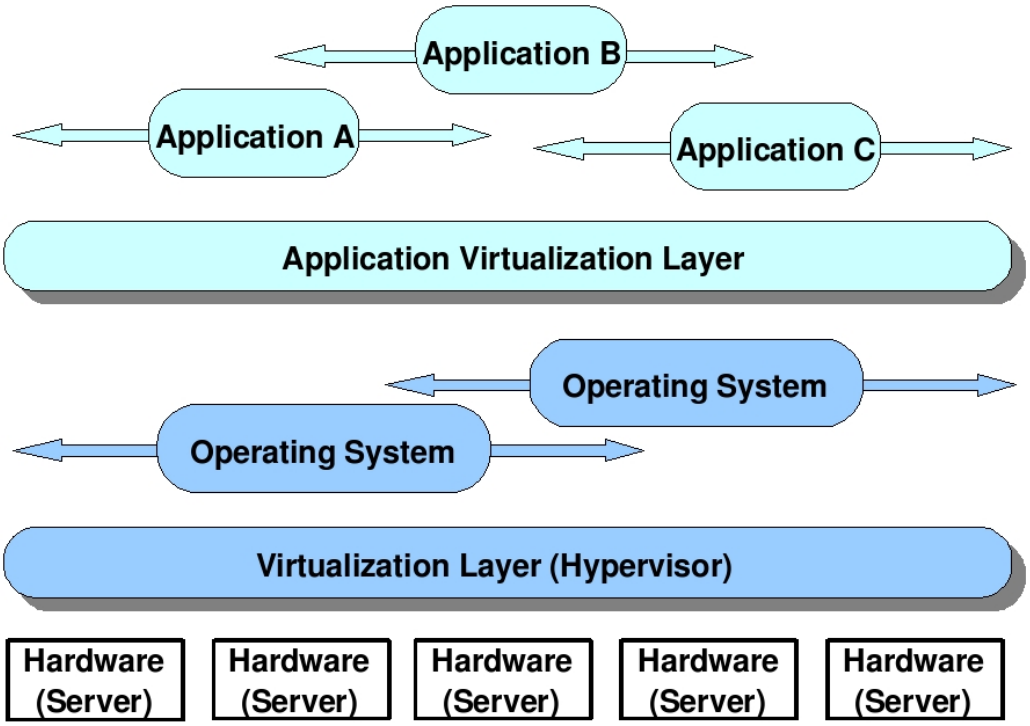

Figure 2. Flexible control room setup. By implementation of two virtualization layers, applications are abstracted from the O/S which in turn is abstracted from the hardware.

The second option uses remote access to applications which are hosted on servers not necessarily directly reachable from the control room network. Ideally, the behavior of such remote applications should be exactly the same as when working with locally installed programs (e.g. start menu entry, desktop icon, access to local disks,

etc.). For this purpose, a centralized secure access framework has to be in place which enables seamless, cross-platform integration of remote applications into existing desktops. In addition, using this framework ensures existing security policies in two respects. One the one hand, it handles all necessary network connections, i.e. no direct connections are established between the control room network and the external network areas where the remote applications are hosted. On the other hand, all data transfer can be encrypted, which means the remote applications can be delivered to control room desktops in a secure way (Fig. 3).

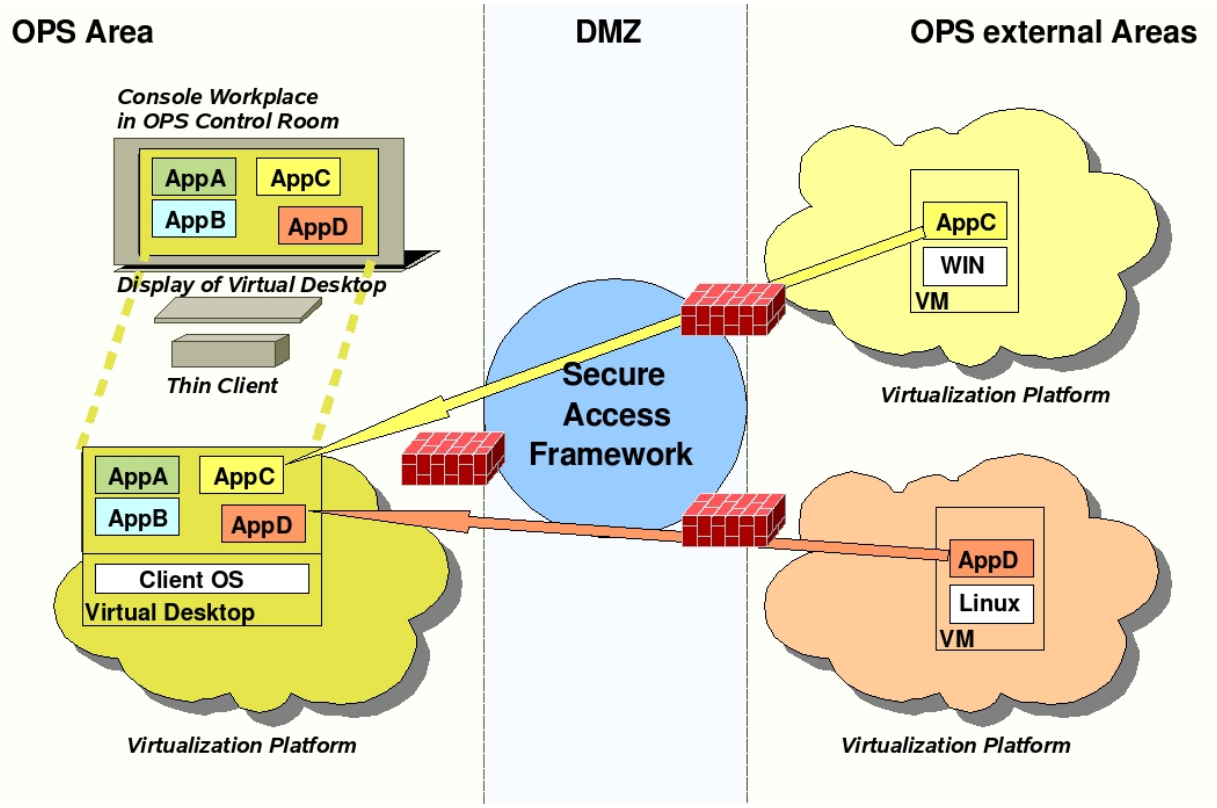

Figure 3. Enhanced application virtualization. Single applications (AppC and AppD) running on servers in external network areas are delivered to the virtualized desktop over a secure access framework.

B.Recent Developments in Virtualization Techniques

Server virtualization is nowadays a well-established system in numerous companies being in place there for already several years.

As servers have become more and more powerful, one is able to virtualize even those services needing lots of performance. Apart from that, optimizations of the hypervisor led to a reduction of the overhead caused by this additional layer. That leads to noticeable improvements especially concerning disk I/O as well as network latency. As the percentage of virtual machines has increased considerably during the last years, many hardware manufacturers came out with hardware (e. g. storage systems or network components) specifically designed for the utilization in virtualized environments. On the one hand this leads to a considerable gain in system performance. On the other hand it brings advantages in administration and monitoring of the hardware since these tasks can now be achieved directly by using the management tools of the virtualization infrastructure being already in place. With mechanisms which allow exact allocation of resources (CPU, RAM, storage I/O, network bandwidth) to each VM, it now can be guaranteed that the virtual systems do not interfere with each other. When using server pools, an automatism is available, that balances the load produced by the VMs between all servers. Beyond that the VMs can be protected by high availability features.

In contrast to server virtualization, desktop virtualization is a relatively new technology which uses the same virtualization infrastructure as the server virtualization. However, there are additional and specific requirements

having to be met to enable the user to work on the virtual desktop without difficulty (e. g. adequate graphics performance). The latest releases of virtualization software provide new features like 3D graphics support for the VMs. Furthermore it is now possible to redirect external devices connected to the client device (e. g. an USB smart card reader) to the VM O/S, so that they can be used in the same way as in a non-virtualized environment.

C.Simplification of Administrative Tasks

All VMs running on top of hypervisors can be administrated centrally with commercially available tools. Those provide a time-saving management possibility; specifically the deployment of new VMs is easy and fast. When new patches or software versions are needed, just the VM template has to be altered. This ensures that all freshly deployed VMs automatically contain all necessary software packages. Furthermore, a snapshot tool allows “freezing” the current state of a VM at any time. This can be very useful when tests (e.g. with a new software version) have to be performed - if the tests have been successful, the VM can be kept running with new software version; if not, it is quite easy to revert to the status the VM was in before the tests. Another feature is the possibility to migrate a VM from a hypervisor on one hardware to a hypervisor on another hardware while it is running (so-called live migration). As a result, downtimes can be minimized or even be avoided completely.

D.Prerequisites for a Successful Virtualization Project

Desktop virtualization requires a stable virtualization platform. If the infrastructure for server virtualization is already in place, it would make sense to use that for desktop virtualization as well. Ideally, virtualization is based on two blade centers housed in computing centers physically separated from each other; as an alternative, one could build up two pools consisting of multiple standalone servers having the same equipment. Data is stored in a centralized, redundant storage system which communicates via FC, iSCSI or NFS. All network connections between blade centers, servers and the storage system support transmission rates of 10 GBit/s and are designed redundantly as well. The client devices are connected to the network using bandwidths of 1 GBit/s or more.

E.Client Devices in the Control Room - Workstations or Thin Clients?

In principle it is possible to use the workstations already available in the control room as client devices for desktop virtualization. A prerequisite for this is the utilization of an appropriate graphics card in the workstations supporting the desired number of monitors to display multiple virtual workplaces in parallel. However, devices sold under the name "thin client" by different manufacturers are much more qualified for this purpose because they show several advantages over the standard workstations.

First of all, the thin clients are more durable and also more failsafe since they do not have rotating hard disks but flash disks. Apart from that, the noise level in the control rooms can be lowered because thin clients work very quietly. Last but not least, the minor power consumption is environmentally friendly and helps reducing costs.

F.Connection Types and Protocols

There are two different ways for establishing connections between the client device in the control room and the virtual desktop in the server room – the first method is using a connection broker and the other one is a direct connection to the target system.

The so called connection broker is an element of desktop virtualization coordinating remote accesses to the target systems. All the intelligence is integrated into the connection broker whilst no information has to be stored on the client side. From the client device, simply a connection to the central connection broker has to be established which then redirects the request to the suitable virtual desktop. Virtual desktop infrastructure (VDI) solutions using a connection broker are commercially available from different producers. Unfortunately most of these systems provide support only for virtual Windows desktops but not for virtual Linux workplaces.

Alternatively connections can be established from the client system in the control room to the virtual workplace directly. This method is less flexible because the connections available to the operators cannot be administrated centrally but the configuration work has to be done separately on every single client device.

A typical connection to a Windows desktop is established using the Microsoft remote desktop protocol (RDP). An advantage of this method is the fact, that all necessary software is already in place after a Windows O/S has been installed. Some commercially available VDI solutions use other proprietary connection protocols (e. g. PCoIP).

For Linux desktops the situation is more complicated. The performance of the X display protocol over the network is too low to allow the users to work on their remote desktops in a satisfactory manner. By using the NX technology this situation can be improved drastically. The NX server components need to be installed in the Linux desktop VM, while the NX client software has to be available in the control room.

In principle, connections to Windows and Linux virtual desktops can be initiated using a simple web browser

which has to be equipped with the appropriate RDP and NX browser plugins.

V. Current State of Virtualization at GSOC and Plans for the Future

In GSOC a virtualization solution based on hypervisors is running stable for more than 3 years. Most of the VMs are virtualized servers with services like dns, ftp, etc. or other project-specific services (SCOS, SATMON, etc.). Up to now, there are only a few VMs containing virtualized desktops. As the centralized storage system is not yet in place, each VM is stored on a local disk of one the servers and can therefore not be easily migrated to another server hardware.

Over the last few months a new virtualization concept for GSOC has been developed, providing as much flexibility as possible to administrators and users and taking into account all the special requirements for desktop virtualization. The next step will be the installation of a redundant 10 GBit/s network infrastructure, to which a centralized storage system and high-performance servers suitable for virtualization will be connected. All VMs including the virtualized desktops will be migrated to this highly flexible virtualization environment at a later time.

The current installations used for testing desktop virtualization include different O/Ses like Windows XP, Windows 7, openSuSE Linux, SuSE Linux Enterprise Server, etc. Connections from the client devices in the control rooms could be successfully established to all of those systems, using either the remote desktop protocol (RDP) for Windows desktops or the NX protocol for Linux desktops. The majority of applications started in the VMs were running smoothly on the client side, only in exceptional cases a performance tuning of the desktop VM was necessary.

Although a setup with a connection broker was also tested, usually all connections were established directly. As a connection broker does not affect the performance the user experiences, it can be added to the existing infrastructure at a later time.

While there are still conventional and virtualized systems side by side at the moment, GSOC is aiming to equip control rooms exclusively with thin clients in the near future.

VI. Conclusion

Modern IT solutions can bring several advantages for operations in the control rooms. By breaking traditional dependencies the flexibility of the systems will be drastically enhanced, especially by using technologies like desktop virtualization and application virtualization. This can solve the problem that a control room is blocked by a single project for a long period of time. While the reconfiguration of the control room systems is a complex and time-consuming task at the moment, operators can switch quickly and easily between different setups like training and simulations when using virtualization techniques.

At GSOC it is planned to establish virtualized desktops as a standard for control room setups.

Appendix A
Acronym List

DLR	German Aerospace Center
GSOC	German Space Operations Center (part of DLR)
VM	Virtual Machine
O/S	Operating System
RDP	Microsoft Remote Desktop Protocol
VDI	Virtual Desktop Infrastructure
IT	Information Technology

References

Proceedings

[1]Knorr, E., Schmidhuber M., "Server Consolidation and Client Flexibility in GSOC Multimission Environment", *RCSGSO 8 Workshop, 2009.*

[2]Schmidhuber, M., Kretschel, U., Singer, T. and Uschold, A., "Virtualizing Monitoring and Control Systems: First Operational Experience and Future Applications", AIAA, *SpaceOPS, 2010*.

Computer Software

[3]VMware vSphere, Ver. 4.1/5.0, VMware Inc., 2011, URL: http://www.vmware.com.

[4]Leostream Connection Broker, Ver. 7.0, Leostream, 2011, URL: http://www.leostream.com.

[5]Oracle Secure Global Desktop, Ver. 4.62, Oracle Corporation, 2012, URL: http://www.oracle.com.