Common Desktop Technology

Martyn Fogg[1]
SciSys UK Ltd, Methuen Park, Chippenham, Wiltshire, SN14 0GB, UK

Claude Keppenne[2]
Eumetsat, Eumetsat Allee 1, D-64295 Darmstadt, Germany

In Ground Segments for existing missions, dedicated workstations have generally been provided to support specific functionality and roles leading to a proliferation of equipment and the need for dedicated office space. EUMETSAT currently have separate control rooms dedicated to specific missions and are looking to revise this concept for METEOSAT 3rd Generation (MTG) and future missions. This paper, written in conjunction with EUMETSAT, summarises the analysis carried out as part of the MTG Common Desktop study which looked at how technology can be used to provide common integrated access into MTG ground segment facilities. The paper considers how different technologies such as web-based technology, service oriented architectures, thick and thin clients and desktop virtualisation can be applied and considers how best to meet the overall operational needs. This includes controlled provision of functionality to a variety of working zones ranging from dedicated mission control rooms to multipurpose rooms, company offices and external locations. This raises significant issues in terms of security, management of software updates, and access to local resources such as data storage, printers and audio devices. The provision of integrated access control management, notification and interaction mechanisms spanning all locations is discussed.

I. Introduction

THE ground segment for operational missions of the complexity of those managed by EUMETSAT is accessed by a wide range of users, including both EUMETSAT's internal users (operations, maintenance and science/product specialists) and their operations partners (ESA, spacecraft manufacturer, external science/product specialists). This covers all Ground segment functions – mission operations, instrument data processing, product extraction and dissemination.

Each user role requires access to a different set of MMIs. In previous generations of the ground segment, dedicated workstations have been provided to support these roles, augmented by user login to restrict access to a specific set of functions.

For future missions including MTG, one possibility under consideration is to provide a common set of desktop infrastructure solutions that allow access from multi-purpose workstations available in a number of different working zones, each with specific security and access control constraints. This would make better use of office resources by allowing some activities to be moved away from dedicated control rooms.

A number of distinct working zones have been identified, including Operations and Backup Control Rooms, Operations Engineering, Multipurpose Rooms that can be reconfigured to support special operations or software and algorithm development, Offices and External Zones that facilitate remote access by internal users.

The scope of the Common Desktop Infrastructure solution may be summarised as:

- To provide access control, including user authentication and management of access rights for all zones.
- To support deployment of the MTG MMIs on multi-purpose workstations, on EUMETSAT's office PC network, and remotely.
- To support common functionality in all zones, including notification and interaction message display.

[1] Software Consultant, Space Division, SciSys UK Ltd. Email: martyn.fogg@scisys.co.uk.
[2] Ground Segment Engineering Group Leader, Programme Development Department, EUMETSAT. Email: claude.keppenne@eumetsat.int.

The MTG Ground Segment is complex and its decomposition (from a user access perspective, shown in Figure 1) can be considered from multiple viewpoints, including:

Functional: classical decomposition into functional components. Individual user's access may be restricted to specific MMI applications or even individual functions within those MMIs.

Environment: an environment is a deployment platform that hosts a set of functions. Different types of environment may host different sets of functions (On-line, Engineering, Reprocessing, Development). Multiple copies of an environment can be used to support different operational tasks in parallel (Operations, Validation, Integration). Users may have differing access rights to the various environments. Depending on user role, access may need to be restricted to a single environment at a time, or they may need access to multiple environments in parallel.

Mission: although the study is specific to the MTG programme, the potential is noted for multi-purpose rooms, office PCs and external access to support multiple missions using the same common desktop infrastructure. In this event, access may need to be restricted at Mission level.

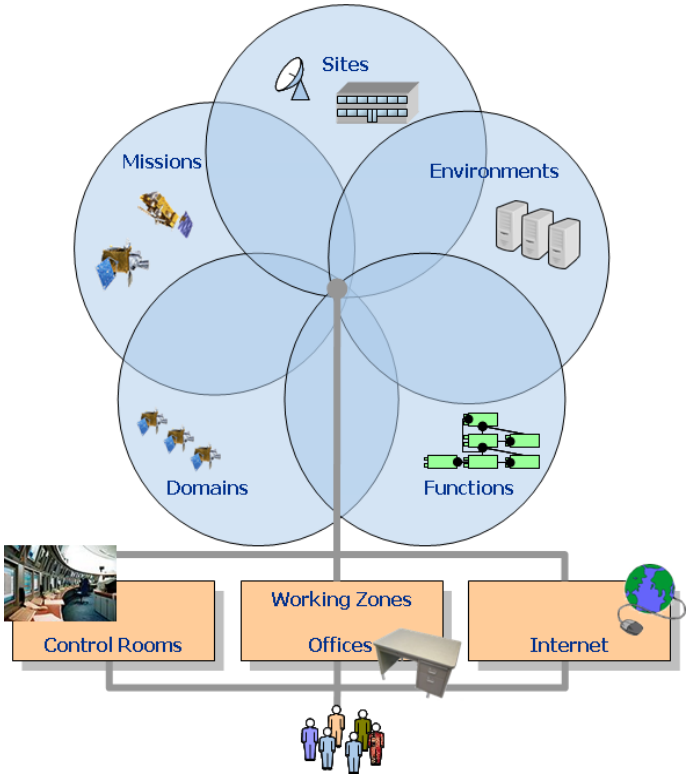

Figure 1. System Context. *The Access to the Common Desktop is required from different working zones with access controlled by reference to Mission, Site, Environment, Domain and Function as well as the working zone itself. The access zones fall into three main categories, Control Rooms, Offices and External, which may each require specific connection technologies.*

Domain: multiple copies of the same function or dataset may exist to support multiple spacecraft or ground station domains. User access may need to be restricted by domain.

Site: some environments will be duplicated at the Back-up control centre. Users may have the same access rights in Control Centre and Backup Control Centre, but local access control should be provided at each site to ensure redundancy. This may imply replication of user authentication and access right databases between sites.

Working Zone: User access will vary depending on the working zone they are located in.

II. Analysis of Requirements

An initial requirements capture and analysis phase was carried out. This included a workshop and use case analysis (Figure 2) to capture the users and uses of the system. A number of key requirements were identified, outlined below.

A. Access

The Common Desktop should facilitate access, subject to authentication and authorisation controls, to ground segment functionality from the different working zones. The information presented should have a similar format and content from all access areas. There is no a-priori allocation of terminals to screens, functions and programmes.

B. Authentication and Authorisation

The Common Desktop should allow or restrict access to ground segment functionality based on the user's role, working zone, mission, facility and domain. This authentication (securely identifying the user) and authorisation (determining the user's level of access) should be configurable and the system must make users aware of which environment they are logged in to. The system should also allow application software to access information about

the user's rights and permissions derived from the login context (user, role, zone etc). This will allow applications to provide fine grained control of functionality.

C. Remote Monitoring

The system should facilitate Remote Monitoring of desktops, with or without the user's knowledge. The user should not be required to explicitly accept remote monitoring, as this may be a distraction from ongoing critical operations. This functionality may only be appropriate for on-line workstations or in a training context, so control over which desktops can be remote viewed is important. It is restricted in its availability; it is to enable viewing of workstations within the Control room from Operations Engineering or Multipurpose rooms only.

It should be noted that the requirement for remote monitoring is for live monitoring of user desktops and actions, rather than post analysis. This is in addition to traceability requirements, which allow post-analysis of system logs.

D. Security

The system should be secure in order to prevent malicious or accidental access to the system. This applies to all zones, including external access. The system will ensure that access operations are traceable to a user and/or role.

E. Repurposing

The system should offer a simple, low cost method of repurposing desktop machines to be used for other roles or missions. This implies the installation of specific software on the desktops should be minimised.

F. Platforms

The system should be portable across a range of operating systems. As a minimum, Linux desktop clients and servers should be supported, as well as allowing access from standard desktop PCs running Windows. Consideration should also be given to support for other operating systems, such as Apple and Android devices, which would allow the possibility of wireless devices in future.

G. Scalability

The system should be scalable, coping with the MTG mission in the first instance with the ability to incorporate other missions in the future. In addition, consideration should be given to allowing existing missions (such as MSG) to be migrated to the same environment should a valid business case exist.

H. Application Independence

The Common Desktop should minimise the requirements on current and future application software.

I. Local Resources

The system should allow the use of local resources at the desktop, such as printers, file transfer and sound. Sound relay is important to ensure that alarms are heard from the remote desktop. Users may also need to extract off-line data, including screen capture, to a normal office environment for analysis.

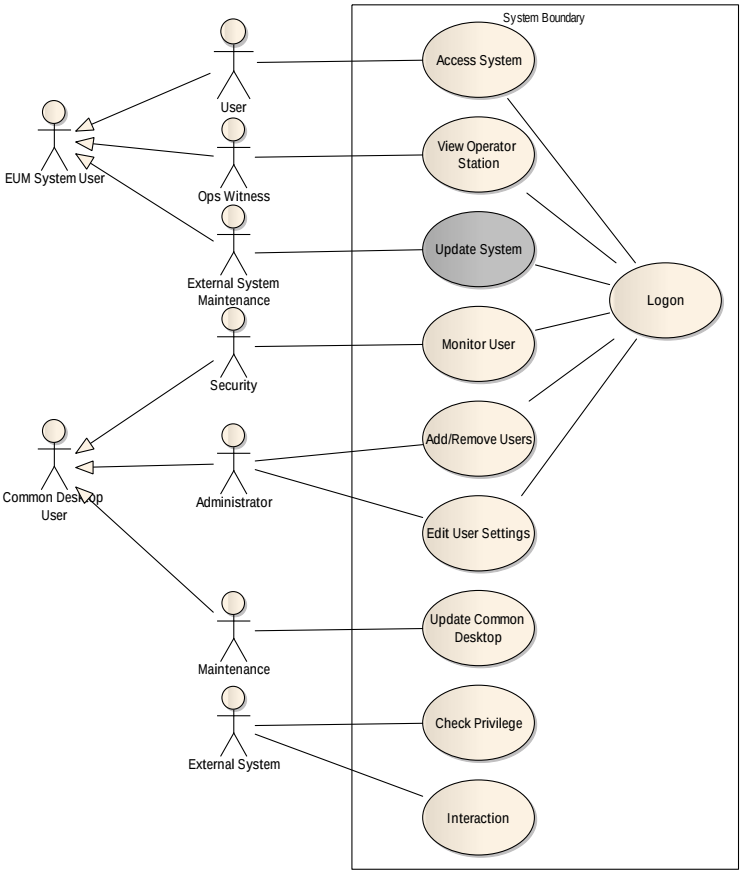

Figure 2. Top Level Use Cases. *A use case analysis was carried out during the requirements phase, identifying the Common Desktop system users and the associated modes of operation of the system. The figure shows the top level Use Cases.*

III. Technology Analysis

After requirements capture, the next phase was to evaluate candidate technology solutions to meet those requirements. Three main areas were investigated: Thick Client Solutions, Web Based Technologies and Desktop Virtualisation. These are discussed in the following sections.

A. Thick Client Solutions

In a Thick Client architecture, client computers provide rich functionality independent of the central server. Constant connection to the server is not always required (although a least periodic connection usually is), as a thick client has the ability to perform many functions without that connection. The clients in this scenario are generally required to be high performance and usually have their own storage and more memory. As a result they tend to have a shorter lifespan and higher cost. Correspondingly however, less demand is placed on servers so reduced server specifications may be possible.

In the Common Desktop environment, applications need to access authentication and environment information, such as user role and zone, in order to control access to features. A Service Oriented Architecture approach could be used to provide a common way for applications to access this information. The use of a Common Access Layer (Figure 3) was proposed, a thin layer of software installed on all clients that provides controlled access to the system and to a common set of services, based on user, role, zone, mission, environment, site and domain. This builds on the approach used for the MSG Central Facility, where a common software layer was developed which combined access control and generic MMI controls, such as the launch menu, alarms and messages and mission status.

In this model, Service Consumer applications, such as Flight Dynamics or Automation, access services, such as Interaction or Monitoring and Control, via the Common Access Layer. An example of services and consumer applications is shown in the diagram.

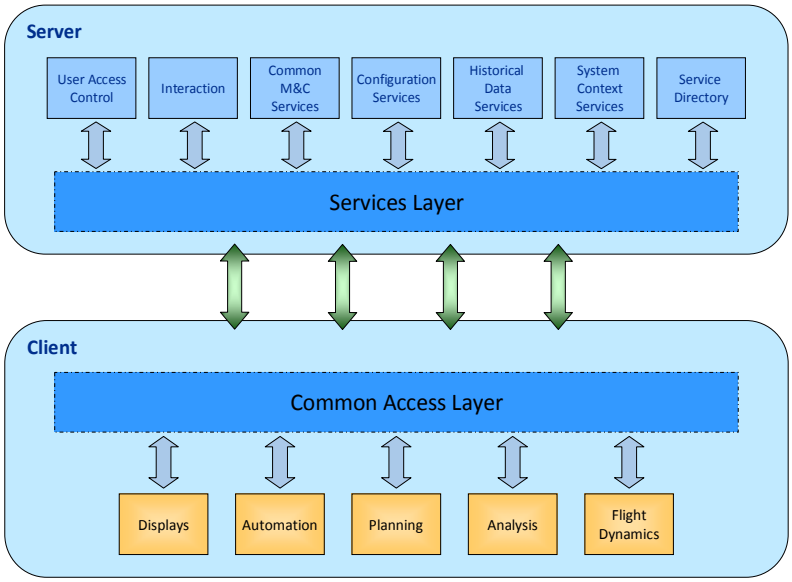

Figure 3. Common Software Access Layer. *A Common Access Layer on the client facilitates access to common services. Example Service Consumer applications are shown, such as Automation and Planning.*

Many of these services are of particular relevance to the Common Desktop, as many of them correspond to needs identified earlier.

User Access control encompasses both Authentication and Responsibility. *Authentication* is tightly coupled to user login; users must login at a workstation to authenticate themselves. Access is controlled at two levels: system access requires a user-id and password and each user, or potentially user role, has an associated set of privileges that can be used to restrict access to services in terms of allowed operations and domains.

Responsibility provides the linkage between user authentication and the Interaction service. The login server maintains a set of responsibility tokens (e.g. for a domain) that are assigned to individual users, assuming they hold the required level of privilege. This is used by Interaction Servers to locate and route operator interactions to the user that currently holds the corresponding responsibility token.

The *Interaction Service* allows an asynchronous notification message to be routed to the responsible human operator, and optionally to receive a response from that operator. For example, this can be used to notify the responsible operator of a significant event, or to prompt the user for input, such as acknowledgment. This service can be closely coupled with the responsibility model to ensure such notifications are targeted to the correct individual(s).

This type of thick client solution may be particularly useful for off-line engineering tasks in the EUMETSAT office environment. In this case the services used may be associated with control of the off-line data transfers between servers and clients. For example,

1. Configuration Management check-in and check-out
2. Access to Flight Dynamics (FD) input data sets (as files) and submission of FD output data sets.
3. Access and submission of Mission planning schedules
4. Data retrieval to support Analysis and Reporting and subsequent submission of reports.

This solution would address many of the requirements of the Common Desktop. Building bespoke software to control access would result in a highly tailorable system which could support future requirements through software modification. Additionally, this approach would provide the improved performance required for highly interactive applications by putting the processing power closer to the user.

However, with this approach, applications would need to implement specific software interfaces in order to be able to request authentication services, rather than more standardised operating system resources. This may increase the cost of software development and complicate procurement of facilities.

B. Web Based Technologies

Web Based Technologies are the first of two Thin Client solutions that were examined. Thin Client architectures feature a shift of processing power from the client to the server, whether that is achieved through Thin Client Hardware or by software architecture. In the case of web technologies, the browser is the 'thin' layer of software that accesses functionality on the server.

Web technologies have now reached a level of maturity such that browser based user interfaces can give just as good a user experience as desktop GUIs for most applications. Advances in recent years, such as AJAX, J2EE, GWT and HTML 5.0, have allowed more and more complex, feature rich solutions to be made available through web browsers so it would now be possible to base access to applications within MTG on this. They provide a number of advantages:

Widely Accessible: Web Applications have the advantage that the application can be made very widely accessible due to browsers being supported almost universally.

No Installation: Browser based software does not need to be installed and requires little or no disk space on the client machine. No network administrator is needed to approve installation of software or to update every client.

Up to date: When the browser is opened, the latest version of the software is automatically accessed on the server. This means that maintenance and updates are done only on the server, making the rollout of new applications or versions far simpler.

Platform Independent: Web applications run in any web browser and are not dependent on the underlying operating system (although browser compatibility issues have to be managed). It can also be argued that this leads to less software bugs since platform dependency issues, such as hardware or environment settings, are a common cause of problems.

Reduced Client Hardware Requirements: Web applications generally reduce overall hardware requirements and Total Cost of Ownership (TCO) as more processing is shifted to the servers. Alongside platform independence, this opens up applications to access from a wide range of devices, such as smart phones, tablet PCs and repurposed PCs. This is an important issue, since traditional desktop applications would generally need to be re-written or ported to mobile devices.

Integration: A large variety of pluggable web applications exist that can be utilised as part of a bespoke application. For example, an application could embed a Google Maps widget to get location data.

The main drawback to web based applications is that they require constant connection to the server and fast and efficient networks. On site this can be managed but for external zone access it may depend on users' home networks.

Additionally, the use of web based solutions places a requirement on current and future applications; all applications must have a web based front end, or at least include a web based component. This presents an issue for any existing applications that are to be used in MTG, for example SCOS would need to have a web component developed. Similarly, new applications would also need a web-based component. However, procuring an application with a web front end rather than a desktop GUI does not necessarily increase the cost and the flexibility gained makes the technology worth consideration.

C. Desktop Virtualisation

Virtualisation technologies have been given a great deal of attention in recent years and they continue to be a growth area. Many organisations have been able to realise cost savings by employing Server Virtualisation, allowing them to reduce hardware costs and energy consumption and manage obsolescence.

More recently, interest has grown in Desktop Virtualisation, which promises similar hardware cost savings. This allows desktop computers or workstations to be virtualised, allowing the resulting virtualized image to be stored on a remote central server (for example within a virtualisation farm or cluster), instead of on the local storage of a remote client. Users interact with a virtual desktop in exactly the same way as they would a physical desktop and can log in remotely to access the desktop from any location and from a variety of devices. When users work from their virtual desktop client, all of the programs, applications, processes, and data used are kept and run centrally.

Figure 4 shows a conceptual VDI architecture. A server hosts a pool of virtualised desktop images, providing the processor and hardware resources. This may be a single server, a rack of blade servers or even a cloud based server farm. The servers are usually located separately from the desktops, so that power, noise and cooling requirements can be properly controlled in each area.

A *Hypervisor* allows multiple operating systems to run on a single hardware host. It acts as a manager of virtual machine instances, controlling the host server processor and resources, distributing what is needed to each operating system in turn and ensuring that the guest operating systems/virtual machines are unable to disrupt each other.

The *Connection Broker* enables the clients to connect to an available virtual desktop image, validating the user and providing a connection according to a predefined policy, group membership or other criteria. The broker monitors the activity of each desktop image, tracking its run state and if a user is currently logged in to it. It can also control the VM state, turning it on or off, or suspending and resuming it.

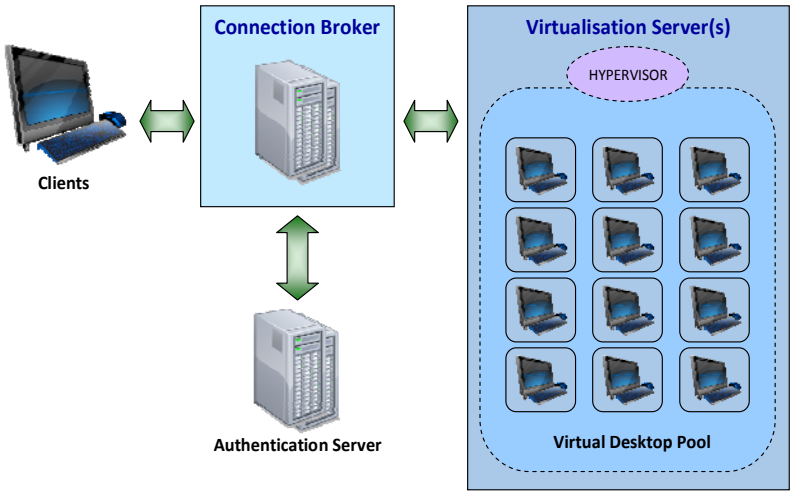

Figure 4. Conceptual VDI Architecture. *A conceptual, Virtual Desktop Infrastructure (VDI) based on the Hosted Virtual Desktop Architecture is shown. Other VDI architectures were examined but were found to be less relevant to the study.*

The Connection Broker authenticates the user via an *Authentication Server*, which can be a separate product such as Active Directory, or may be included as part of the connection broker. Connection brokers are usually arranged in dual redundant pairs with automatic failover, to ensure that there is not a single point of failure. Some connection brokers offer more functionality, such as secure VPNs to secure the remote desktop network traffic.

For access to the desktop, a variety of devices can be used. Commonly either dedicated thin client hardware or repurposed PCs are used. For thin clients, a Thin Client operating system is needed which allows the desktop to boot and to communicate with the broker, relaying screen updates and user.

Using this model, each virtual desktop does not require its own hardware, operating system and software. In common with server virtualisation, desktop virtualisation generally reduces hardware costs significantly. Additionally using desktop virtualization can lower the cost of deploying applications and can reduce downtime in the event of a server or hardware failure.

The application of Desktop Virtualisation to the MTG environment would address many of the issues outlined in the requirements analysis. Solutions exist that allow a common desktop view to be shown across all zones, subject to authentication.

In common with browser based solutions, Desktop Virtualisation is highly dependent on network performance. This is not usually an issue on site, where high performance networks are commonplace, but for remote access from external zone areas usability can suffer if broadband connection speed is low.

IV. Technology Trade-Offs

Each candidate technology was analysed with respect to its applicability to the requirements outlined earlier. The table below shows a high level trade off summary of the findings.

Although this comparison is in some ways simplistic, as often the qualities of the technology depend on the exact implementation, it does highlight that Thick Client and Web Based and solutions each have disadvantages that could make them unsuitable for the Common Desktop. For example, Thick Client requires software to be installed on the client and this may be a problem for the office and external zones, where there is limited control of application installation by operations staff. Web Based solutions require a web front end, which would place requirements on current and future applications, potentially increasing cost. For these reasons, Desktop Virtualisation was recommended as the most appropriate solution for the Common Desktop.

Technology	Advantages	Disadvantages
Thick Client	Highly tailorable. Highly maintainable. Greater control of security. Allows some degree of offline working.	Software installed on all clients. Would require modifications to existing systems and requirements on future ones. Higher client hardware requirements.
Web Based Solutions	Widely accessible. Platform independent, highly portable. Uses open standards. Does not require specialist software on client. Allows integration of third party plug-ins. Access from large variety of client devices.	Requires web front end for applications, present and future. Requires constant network connection.
Desktop Virtualisation	No changes to existing applications. Minimises requirements on future apps. Does not require specialist software on client. Allows gradual migration. Allows use of low cost thin client hardware.	Requires constant network connection. Increases server requirements.

At this point, further analysis of the application of Desktop Virtualisation to the Common Desktop was carried out. There is a wide variety of vendor solutions available and a technology survey was done to evaluate the best fit for the requirements. Protocols and desktop client hardware options were examined first as an aid to understanding the available offerings and a feature summary was produced to compare and contrast them.

The analysis showed that there is little to differentiate the market leaders in terms of functionality. Almost all major vendors provide support for the common VDI architectures and support for multiple client operating systems, multiple monitors, file transfer, sound and local peripherals.

V. The Remote Access Concept

Although the solutions examined so far in this study were well received, as the implications of the scope and requirements became apparent there was a view that too much coupling between contractual elements and too much complexity was being introduced into the system as a whole. As a result, the Remote Access Concept was proposed.

The Remote Access Concept, shown in Figure 5, involved the partitioning of functionality into zones. Control and Operations Room functionality is placed in a Secure Zone, available only from within dedicated rooms at EUMETSAT with access controlled by a firewall. Engineering functions are put into a separate lower security area and can be made available in EUMETSAT Offices and externally via the internet, subject to the correct authentication. The functionality made available remotely is now restricted to the engineering functions such as Operations Preparation, Analysis and Reporting and offline monitoring. Any transfer of data from the lower security area into the secure zone would need to be carefully controlled from within the secure zone itself. For example, if Mission Plans were generated within the lower security area, there would be an explicit activity on the part of an operator within the secure zone to transfer the plans into the secure zone once they have been verified.

This approach significantly simplifies the architecture and requirements without compromising security or accessibility. The focus has changed from an integrated access system to concentrate mainly on client components

that access functionality in the Engineering Zone remotely. Remote Desktop technologies facilitate exactly this and were therefore examined in this context.

Remote Desktop technologies relay screen updates from host machines to remote clients and keyboard and mouse input in the other direction. This allows viewing and remote control of a desktop from another location, subject to authorisation of the host machine. Remote Desktop would allow users in the External and Office Zones to connect remotely to desktops in the DMZ and to view and control them, having access to all of the same programs, files, and network resources.

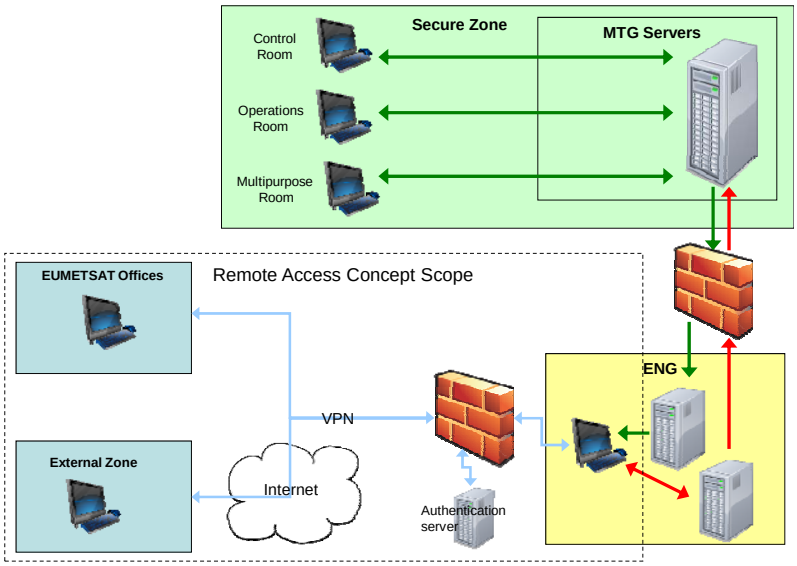

Figure 5. The Remote Access Concept. *Operational Monitoring and Control is decoupled from Engineering by the use of zone portioning. Green arrows represent data that is provided from the Secure Zone into the ENG environment, e.g. monitoring data. There is no feedback path. Red Data represents data generated in the Engineering zone, e.g mission plans. This*

The performance of the remote connection is crucial and selecting the right products and protocols may make the difference between the Remote Access concept being a very cost effective business tool and being virtually unusable. Remote Access may be needed from an Office at the EUMETSAT premises or from across the internet so any solution must be usable with a wide range of performance characteristics. A large number of Remote Desktop products are available and in order to differentiate them a performance analysis was carried out.

The Performance Evaluation compared the performance of RDP, NX, VNC and X11 protocols over several test scenarios, intended to simulate real-world usage:

Idle: The performance was tested under no-load conditions.

SCOS and APEX: The SCOS Mission Control System controlled by the APEX automation product was used to run sample procedure editing and execution test scenarios. APEX and SCOS were connected to a simulator to provide telemetry and commanding simulation. This test involves both user input and screen update so gives a good feeling for responsiveness.

Video Replay: A video was replayed over the Remote Desktop connection in order to test high load performance. Displaying video is a particularly demanding application since it requires a large amount of data to be transferred across the network and displayed very quickly. Network delays and missing packets are made more apparent when the video stutters or reduces resolution.

Using a network simulator and VPN, a variety of different network conditions were simulated, ranging from 100 Mbit/s to 1.5 Mbit/s upload and including simulation of different packet loss and latency conditions. A mixture of objective and subjective tests were then applied. For example, network usage between the client and host was measured for each protocol during each scenario. Additionally, video quality was subjectively measured, based on factors such as the perceived frames per second displayed, the resolution and the whether the video played in real time or not. A selection of results is shown in figures 6 and 7.

The results in general showed that under good network conditions, all protocols performed very well, being responsive to the user and displaying video in good quality. The network usage varied greatly between the protocols, with X11 demanding very high

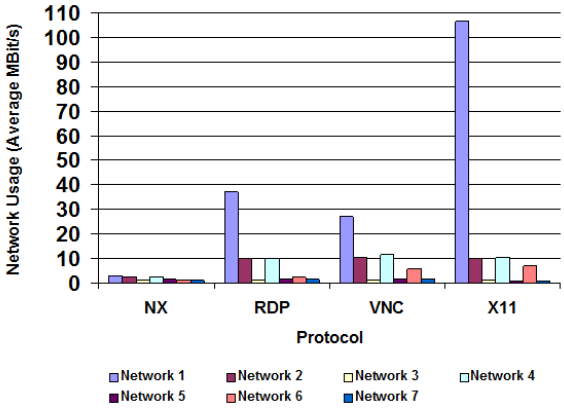

Figure 6. Network Usage during Video Tests

usage and NX very little, but this did not reflect in the usability when the network was high performance.

When network conditions were difficult however, the performance started to vary between the protocols. X11 became unusable at 1.5 MBit/s both for displaying video and in terms of responding to user input. RDP and VNC performed better, but did show slightly lowered performance displaying video. NX performed the best by far, not suffering any real usability issues and being able to show video even at the lowest network limits.

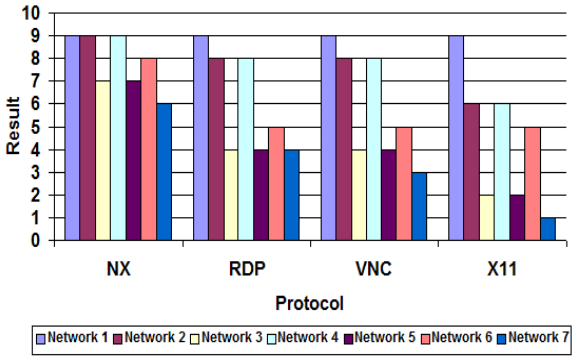

Figure 7. Video Quality by Network and Protocol

VI. Conclusion

The needs of a modern ground segment are many and varied and providing secure, reliable access can be a challenge. A wide range of users require access to a wide range of MMI subject to complex access control rules. This includes users who access the systems remotely.

The study provided a generic analysis of the requirements for the Common Desktop before examining a number of technology solutions that could meet the requirements identified. In this case, Desktop Virtualisation was found to be the most suitable solution, mainly due to the ability to deploy it without updating existing applications and without installing bespoke software on the remote clients. In other cases, SOA or Web Technologies may provide the most suitable solution. As an alternative, the Remote Access Concept could be applied which reduces complexity and coupling without sacrificing security or utility.

The subsequent Remote Desktop performance analysis showed that there are significant differences between the protocols tested. For high performance networks, any of the protocols give good performance. However, where network conditions are difficult, the choice of protocol and product becomes important for usability.

Appendix A
Acronym List

A&A	Authentication and Authorisation
AJAX	Asynchronous Javascript and HTML
ESA	European Space Agency
FD	Flight Dynamics
GWT	Google Web Toolkit
HTML	Hypertext Markup Language
J2EE	Java 2 Enterprise Edition
MMI	Man Machine Interface
MSG	Meteosat Second Generation
MTG	Meteosat Third Generation
PC	Personal Computer
SCOS	Spacecraft Control and Operations System
TCO	Total Cost of Ownership
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network