

Accommodated Checkout and Mission Control and Data System

M. Hobsch¹, Dr. F. Cossavella² and G. Morfill³

German Aerospace Center, Oberpfaffenhofen (DLR), 82234 Wessling, Germany

S2TEP-1 is the first in a series of satellites using the Small Satellite Technology Platform, in short S2TEP. It is developed by the Institute of Space Systems of the German Aerospace Center (DLR) and it will be operated by the German Space Operations Center (GSOC) in Oberpfaffenhofen, Germany. In order to accommodate to the overall low mission costs and high mission risk, a lightweight approach based on a flexible and (partly) autonomous Ground Segment (G/S) has been foreseen. Synergies with other satellite missions at GSOC or with the Central Checkout System (CCS) will be used wherever applicable and productive. A high degree of automation shall be assured. As the desired degree of external interaction from the customer exceeds that of any mission operated by GSOC so far, a Remote Control Center (RCC) has to be established, from where anomaly recovery operations and special payload campaigns can be performed. The focus of our approach lies on cost effectiveness, a shorter development time, user-friendliness and reusability. A high level of security is not required by the project, nevertheless an adequate level of reliability and security is provided. Three designs that meet these requirements are described and discussed in this paper, together with the constraints that arise from implementing them within the current network infrastructure at GSOC. The chosen design for the Central Checkout and Mission Control and Data System is presented: the final approach results in a system built in a nearly traditional way integrated in the multi-mission environment of GSOC.

I. Introduction

The German Aerospace Center (DLR) pursues the objective to develop a cost-effective satellite platform for in-orbit demonstration of technology and for serving small scientific payloads. S2TEP-1 is the first in a series of satellites using the Small Satellite Technology Platform, in short S2TEP [1]. The first satellite of the S2TEP platform will be in the micro-satellite class, to be launched not earlier than mid-2020 and to be operated at least for one year. This platform will be used for technology verification and -sustainability and it will provide standards and fundamental services for scientific payloads. The micro satellite platform S2TEP has a close connection to DLR's already existing small satellite program CompactSat and its first mission Eu:CROPIS, which is scheduled to be launched by the middle of 2018. Technologies developed for S2TEP will also be used on the CompactSat platform and technologies which are flown on CompactSat as secondary payloads can later be flown on S2TEP as critical bus components [2].

The ground segment (G/S) will be designed in such a way that it can be easily re-built for future follow-up missions.

Resulting from the mission requirements and operations concept, currently available system designs cannot be entirely re-used one to one. A partially new concept had to be developed by the Mission Control and Data System (MCDS) team that is responsible for the software used for Monitoring and Control Systems and Offline Data Systems at the German Space Operations Center (GSOC). Since the S2TEP-1 mission constraints to the ground segment are, in terms of required up- and downlink times, data provision times and especially reaction times, lower than for most other missions operated by GSOC, the main design driver has been the integration of this newly developed concept into the multi-mission context at GSOC. Massive reuse of existing software enables operations at moderate costs while still offering high quality of services. The ground segment is designed to enable safe and successful operations throughout the entire mission duration.

¹ Team Lead Mission Control and Data System Group, S2TEP Project System Engineer, DLR/RB

² AOCS Subsystem Engineer, S2TEP Project Manager, DLR/RB

³ Eu:CROPIS Project Manager, S2TEP Flight Director, DLR/RB

Whenever possible, commanding during the mission will be based on flight procedures. A large fraction of the flight procedures will be developed by the satellite manufacturer as test procedures during the Assembly, Integration & Test (AIT) execution. For this reason, the ground segment will provide a Central Checkout System (CCS) mostly similar to the later mission commanding system, together with a test procedure development, execution and documentation tool that has been already used successfully during the Eu:CROPIS AIT.

This paper discusses the constraints deriving from customer requirements and the mission operations concept. After introducing the design of a default Mission Control and Data System at GSOC, three new design approaches are described and assessed. The final approach chosen for the MCDS and CCS of the S2TEP-1 satellite mission is presented. A short conclusion closes this paper.

II. Constraints for the Ground Segment

More and more customers desire a greater flexibility of satellite control centers in terms of lower complexity of the monitoring and control system and versatile possibilities to interact with the spacecraft. This may be even accompanied by reduced security requirements. This is valid for simple, scientific missions as well as for commercial and complex missions. This is in contradiction with the traditional infrastructure of a satellite control center and with the growing complexity of the space segment and its missions. The amounts of telecommands, telemetry, and payload data that must be processed, displayed and distributed are increasing significantly. System engineers designing the S2TEP-1 MCDS System are facing the same challenges.

The S2TEP-1 ground segment has to be implemented in the multi-mission environment of the German Space Operations Center in Oberpfaffenhofen, Germany, in order to use already existing infrastructure and software. Synergies with the Eu:CROPIS project, which will also be operated by the German Space Operation Center and was also developed by DLR-RY, shall lead to a minimal amount of effort and costs.

S2TEP focuses on cost-efficiency and short development times to achieve frequent and more cost-effective access to space for smaller scientific payloads and technology experiments. Using synergies and already existing ground segment components becomes a crucial concept. Therefore nearly all S/W components from the Eu:CROPIS MCDS will be used as-is. Adaptions will only be implemented if the improvement fits to the multi-mission philosophy of the software group or if the project waives its low-cost approach and pays for them.

During routine operations, the ground segment will be operated by two operations team members who have the role of Flight Directors (FLD) and are responsible for the organization and execution of the routine operations of the mission. The ground segment team support is granted only during office hours. During weekends and in case of unavailability of all FLDs, the Satellite Support Team (SST) is responsible for the safety of the spacecraft. The Flight Directors, thus, will be supported also during the routine operations phase by the satellite manufacturer. During all mission phases, the responsibility for the spacecraft safety will be shared between the ground segment and the space segment teams: the responsibility for the safety of the spacecraft in nominal situations lies with the ground segment. Spacecraft anomalies occurring for the first time will be analyzed by the satellite manufacturer that will perform dedicated recovery actions or advice the ground segment on necessary actions. Therefore, the G/S needs to provide a possibility for commanding from external premises in real time. The satellite manufacturer will have command capability from his site and a Remote Control Center (RCC) will be established.

In contrast to the external commanding of the manufacturer, providing real time telemetry to external partners is a well-known and common use case. A tool will be provided to the satellite manufacturer and DLR internal payload teams to monitor real time telemetry during a ground station contact, as well as a tool to display historical telemetry.

Although DLR-RY will be granted full commanding possibility through the RCC, all standard security requirements for a satellite mission remain applicable, i.e. no third party shall be able to command the satellite. As mentioned before, the S2TEP-1 mission will be integrated in the multi-mission system of the German Space Operation Center. Thus, it must be avoided that other missions currently operated by GSOC could be harmed by any (security) issue within the S2TEP-1 system.

During the routine operations phase, an automated commanding process [3] will be established. Files that ought to be uplinked during a ground station pass are submitted 15 minutes before the pass and are then automatically uplinked during the pass. Inputs to the automated commanding system can also be automatically generated and inserted into the uplink-process, for instance the generation of transmitter switches, housekeeping, and payload data downlinks, the so-called background sequence. The automatic commanding mode relies on a purely flight procedure based commanding.

A Central Checkout System is provided by the ground segment to the satellite manufacturer to ease the spacecraft AIT activities and connect to the space segment TM/TC front end. The design and S/W components to be used are identical to the system build for routine operations. Therefore the following considerations about the MCDS are also valid for the CCS. The intensive use of MCDS components in the checkout system is an additional pre-validation of the entire remote commanding system: mission specific configurations will be

already tested at the integration site and potential errors or problems thus detected early in the ground segment development phase.

The Flight Control Procedure (FCP) database is managed by means of the ProToS tool [4] which is linked to the TM/TC database, the so-called Mission Information Base (MIB). The procedures prepared by GSOC and DLR-RY include both standard and contingency procedures. Flight Procedures are subject to version control. A large fraction of the flight procedures will be developed by the satellite manufacturer as test procedures during the Assembly, Integration and Validation (AIV) execution. Flight procedures that become necessary for the Launch and Early Orbit Phase (LEOP) and routine operations which are not available as a by-product of satellite AIV will be generated by the ground segment together with the spacecraft manufacturer.

In order to ease software and hardware maintenance, only few S/W tools will be installed and located at the RCC in Bremen. As best, all S/W tools will be hosted at GSOC and only remote access is granted to the operator in Bremen. Any potential issue can then be easily handled by the S/W provider (the Mission Control and Data System team) or the hardware provider (the Facility and Communication System department at GSOC).

As S2TEP-1 is a low budget project and the S/C is required to survive at least two weeks without any interaction from ground, no redundancy is planned. Moreover, since the system will use mainly virtual machines, should any component in the G/S fail to work, it can be replaced or re-installed within this reasonable timeframe.

III. Design of the System

A. Discussed MCDS Components

In this section, the S/W system provided by the ground segment is reduced to four main S/W modules: The SLE Switch Board (SSB), the GSOC Enhanced Command and Control System for Operating Spacecrafts (GECCOS) [5], the telemetry display system Satmon [6] and the Procedure Tool Suite (ProToS). Reducing the whole system to these four modules, allows the description of the design principles in a more understandable, though still meaningful, manner. The connection from the RCC in Bremen to Oberpfaffenhofen will be realized via a VPN Tunnel, which has been already tested during the Eu:CROPIS AIT phase. As previously mentioned, the Central Checkout System (CCS) needs to be designed in the same way as the routine operations system. Therefore, the considerations done in the following chapters are valid for both. The dedicated S/W modules will be described afterwards.

SSB: The SLE Switch Board (SSB) service establishes the connection between the satellite Monitoring and Control System (MCS, e.g. GECCOS) and the ground station using the SLE protocol. The SSB can receive telemetry flows from the different stations (mostly as SLE PDUs) and converts them into NCTRS Format (Network Command Telemetry Routing System), a data format understood by the MCDS/GECCOS. The SSB is able to receive several telemetry flows in parallel and send them to different MCDS instances. In the other direction, the SLE receives telecommands from the MCDS software (in NCTRS format), converts them into SLE PDUs and sends them to the corresponding station (only one at a time). The SSB is a standard element of multi-mission environment of GSOC and will be used as-is.

GECCOS Server and Client: The TM/TC system to be used for S2TEP-1 is the GSOC Enhanced Command & Control system for Operating Spacecrafts (GECCOS), which is based on SCOS 2000. SCOS 2000 is developed by ESA and is in its core components free for use by other agencies. The SCOS baseline version is 3.1. It is continually maintained and improved by GSOC as the GSOC product GECCOS. It has been used for other GSOC missions (CHAMP, TerraSAR-X, TanDEM-X, FireBIRD, Eu:CROPIS). The version to be used for S2TEP-1 is derived from the latest multi-mission branch with appropriate configurational changes. The S2TEP-1 CCS will also be built with GECCOS as core component.

Satmon Server and Client: Satmon is used to monitor telemetry in real-time and provides a playback function for telemetry received during real-time passes. This application is jointly developed with an external supplier. It is used in all GSOC missions as the telemetry user interface. The adaptation to GECCOS has already successfully been demonstrated for the GRACE, TerraSAR-X/TanDEM-X, FireBIRD and Eu:CROPIS missions and many others.

ProToS Server and Client: ProToS is a tool that offers a graphical frontend for procedure development, a procedure-based automated commanding interface to GECCOS and procedure validation and reporting mechanisms. It has been developed by the mission operations department (RB-MIB) of the German Space Operation Center. As an eclipse RCP tool it can be deployed on a system with a java virtual machine. Procedures are stored in a repository under version control. Several versions of the MIB can also be managed inside ProToS. For downwards compatibility, ProToS can import and export flight procedures in a generic XML format that is used by the Manufacturing and Operation Information System (MOIS) [7]. Procedure templates can be exported as pdf for convenient reading and for test documentation purposes a pdf export of as-run

procedures is also possible. ProToS also generates Saved Stack Files (SSF) files, which can be loaded into the GECCOS system for command execution.

B. Default Mission within the multi-mission environment

GSOC operates several missions in a multi-mission environment. Multi-mission aspects are present in various sub-systems, such as the in-house network, the ground station network and software tools. Within the control center, three different local area networks (LANs) are defined. For this paper, only the Operational LAN (called Ops-LAN) is relevant. It includes the MCS and therefore the high security network area. It is physically separated from other networks and only very limited access from outside is permitted. File transfers are allowed only over specific FTP server located in the so-called DMZ (Demilitarized Zone). In principle a connection over the firewall is only allowed for connections that are established from the Ops-LAN to the DMZ and not vice versa. The mentioned DMZ is the typical separator between different LANs. It consists of another network part with two firewalls protected entry points. DMZs typically contain only firewalls and FTP servers, in case of some specific application the outermost DMZ may, however, also include some application server to provide dedicated services to the outside world. The whole MCDS is usually located in the Ops-LAN [Fig. 1]. Communication over its network borders is only established to the SSB in order to send commands or receive telemetry.

This default design does not meet the requirements for the S2TEP-1 MCDS, as direct interaction with the satellite would then be only possible from the Ops-LAN. Third parties – as payload engineers – would be able to interact indirectly via the operational engineers at GSOC or more complicated ways. This design is then not feasible for S2TEP-1, as only two FLDs are present at GSOC and contingency operations shall be done also from the Remote Control Center in Bremen. Consequently new approaches need to be developed.

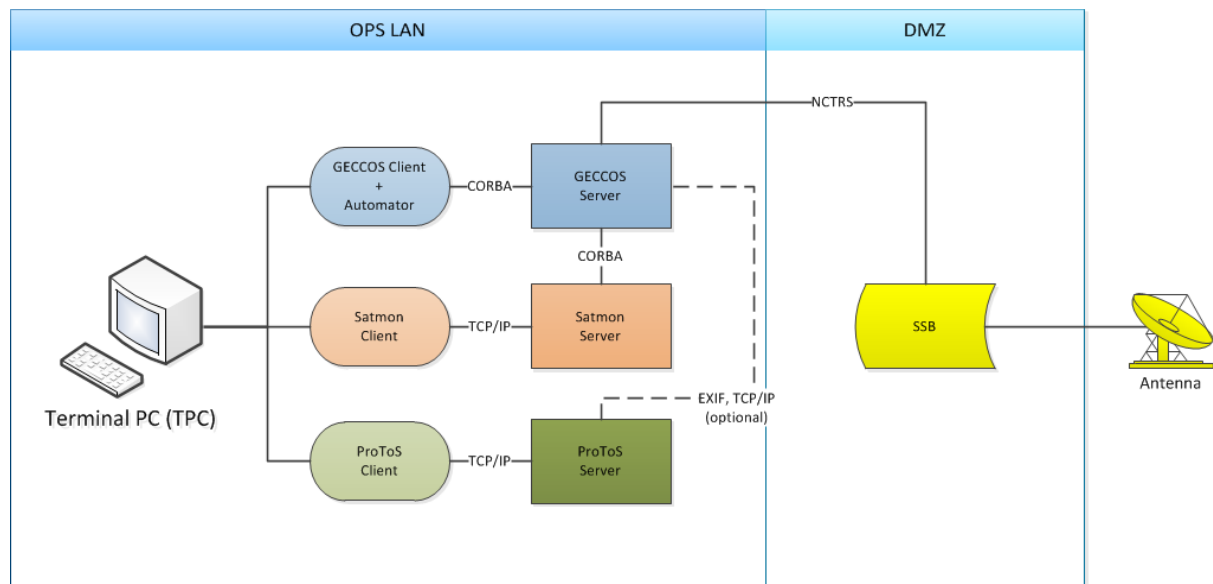


Fig. 1 Default design of an MCS in the multi-mission environment at GSOC

C. Option 00

The first design option consists of only one operational chain located in the DMZ. All servers can be accessed by clients either located in the Ops-LAN at GSOC or at DLR-RY. In this way, both operational parties are able to access the same servers. The communication between clients in the Ops-LAN and the DMZ (and vice versa) needs to be realized through firewalls. Connecting the remote servers in the DMZ with the clients in Bremen over the Wide Area Network (WAN) can be realized technically by a VPN tunnel which has been already tested during the Eu:CROPIS AIT phase. The Eu:CROPIS CCS has been connected to servers at GSOC in the same way. Unfortunately this has not been tested for routine operations.

The operational engineers at GSOC would be able to command the satellite from their accustomed environment. Integrating only one server chain meets the low cost approach of the project and eases software and hardware maintenance effort. Due to common servers accessed by all parties no synchronization of telecommand and telemetry is necessary. Information stored on or provided by the servers is accessible by all parties. Any needed share point for additional information can be located in the DMZ as well. Also, with only one common server for commanding the satellite it is simpler to restrict the amount of clients that are commanding the satellite in parallel. This is the favorite design by the GSOC operations and system engineers.

Having the servers located in the DMZ and communicating over network borders poses however security matters. Establishing connections from the DMZ into the Ops-LAN is currently not allowed due to security restrictions. GECCOS uses the CORBA protocol for communication with its clients by establishing connection in both directions. In addition, at least three connections between the Ops-LAN and the DMZ would have to be opened [Fig. 2]. This means that at least three connections would lower the security measures against hazardous harm to the Ops-LAN. These security gaps are even worse considering that nearly all other satellite missions are flying within the multi-mission environment and would be affected directly by any S2TEP-1 security issue.

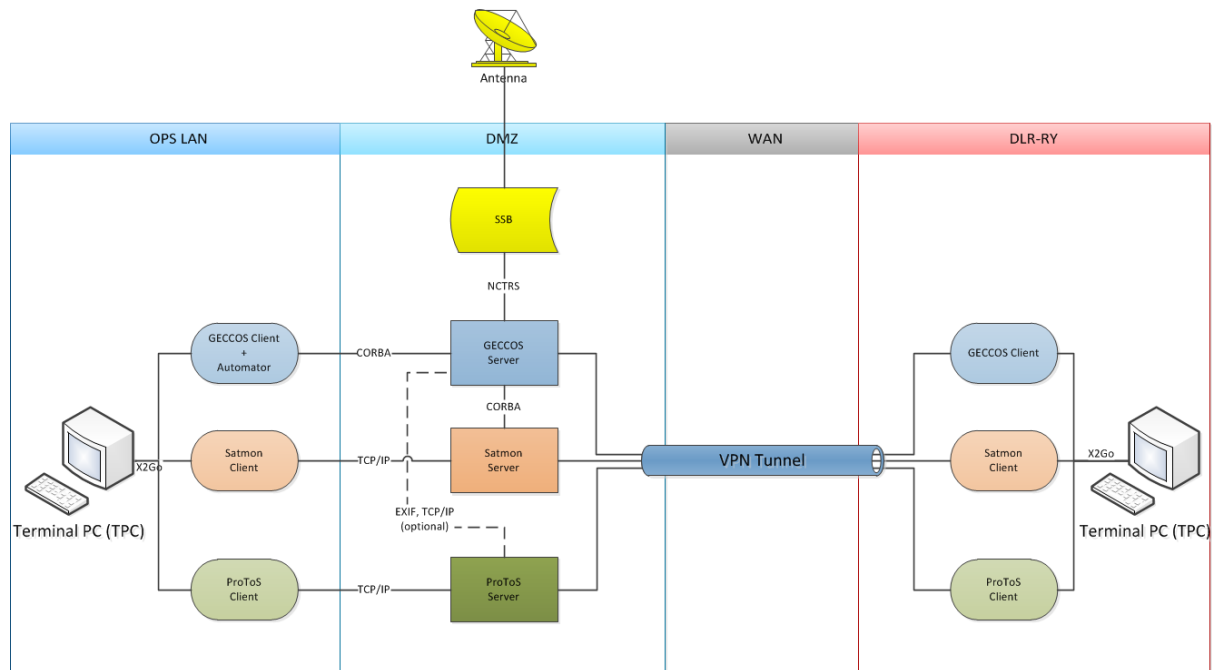


Fig. 2 Option 00: One command chain, clients at GSOC and DLR-RY

D. Option 01

According to this design, two separate operational chains are implemented. One chain is located completely in the Ops-LAN at GSOC. The second one is located in the DMZ also at GSOC. Operations engineers from DLR-RY are able to connect to the servers of the second chain via a VPN Tunnel [Fig. 3]. The operator running the SSB can actively choose which chain is connected to the ground station. Thus, it is assured that only one party can command the satellite at a time and parallel commanding is avoided. If there is any need for a spontaneous switching of the chains, the operator is available twenty-four-seven at GSOC.

The operations engineers at GSOC are able to command the satellite from their accustomed environment. No forbidden connection is established over the network borders between the Ops-LAN and the DMZ. Thus the risk of security flaws is minimized.

On the other side, providing GSOC and the RCC with the same information is very challenging with this design. Any command that has been sent or any procedure that has been generated on one chain must be synched with the other chain, otherwise the other party has inconsistent information about the operational status. This information must be doubled over network borders technically or by operational procedures. Telemetry is not affected by this problematic, since it is streamed to all GECCOS servers in parallel by the SSB, anyway.

Not only information is doubled: in this design, all servers, all clients and all software need to be duplicated. The effort for integration, testing and maintenance during the routine phase is significantly higher than for option 00.

As mentioned in section B, the DMZs typically contain only firewalls and FTP servers and not fully operational server chains. It is still an open point if the GSOC DMZ is capable of providing enough capacity and computing power for operating an operational MCDS chain.

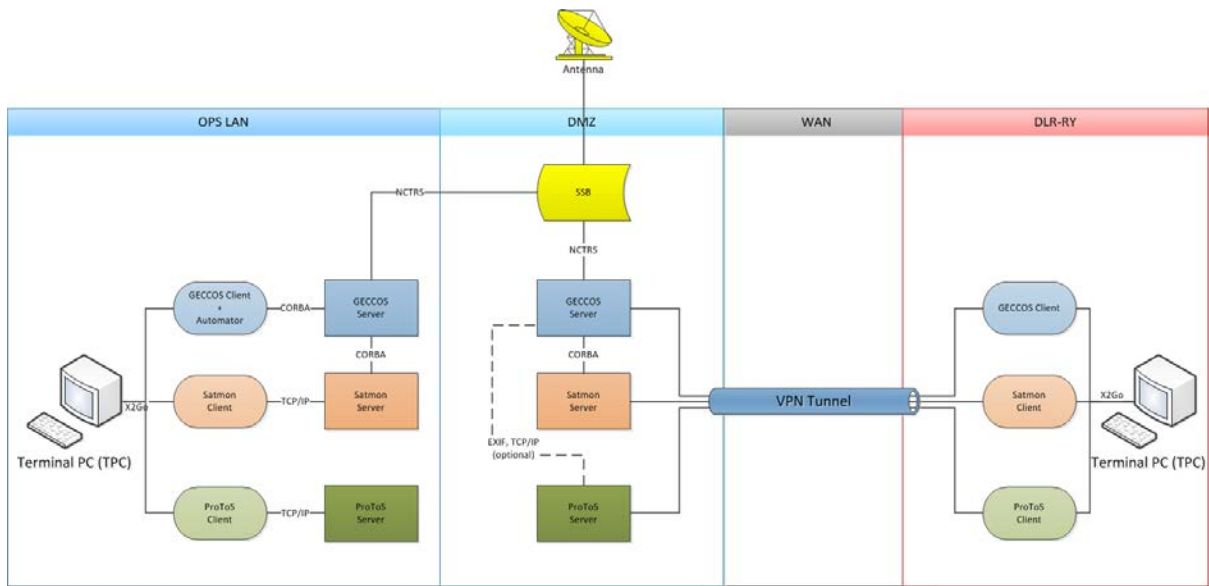


Fig. 3 Option 01: Two command chains, clients at DLR-RY

E. Option 02

The third design proposal resembles the first one. There is only one operational chain that is located in the DMZ. Also the clients are located there. They can be accessed by GSOC as well as by RCC via remote connections using remote desktop software, e.g. X2Go⁴ or NX Nomaschine⁵. The remote connections from the RCC would use a VPN Tunnel to connect into the DMZ.

The operational engineers at GSOC are able to command the satellite from their accustomed environment. It is transparent for them whether the client session they work on is running on a server in the Ops-LAN or in the DMZ. Even for operators sitting in the RCC working with a session that runs in the DMZ there is no difference. As there is only one client it is assured that only one party can command the satellite at the same time. Monitoring the satellite is possible for all parties at the same time by using Satmon. A process for taking over sessions must be established technically or organized operationally. Integrating only one server chain meets the low cost approach of the project and eases software and hardware maintenance effort. Due to common servers accessed by all parties no synchronization for telecommand and telemetry is necessary.

Using X2Go for terminal server software is well proven within the Ops-LAN (see section B). Terminal server connections over network borders through firewalls and especially over the Wide Area Network (WAN) are not fully tested yet, so GSOC needs to gather experience concerning this topic. In addition, only few other terminal software solutions are available for such remote connections.

As mentioned in section B, the DMZs typically contain only firewalls and FTP servers and not fully operational server chains. It is still an open point if the GSOC DMZ is capable of providing enough capacity and computing power for operating an operational MCDS chain.

As X2Go is an open source remote desktop software that uses the NX technology protocol, it gives remote access only to the Linux graphical user interface. It provides secure remote sessions via the Secure Shell protocol (SSH). Thus no possible security flaw will be introduced in the system. This design in principle is similar to new concepts currently in development at GSOC [8]. Changing the remote connection protocol to HTTP may make the access and remote operations more comfortable in future.

⁴ <https://de.wikipedia.org/wiki/X2Go>

⁵ https://de.wikipedia.org/wiki/NX_NoMachine

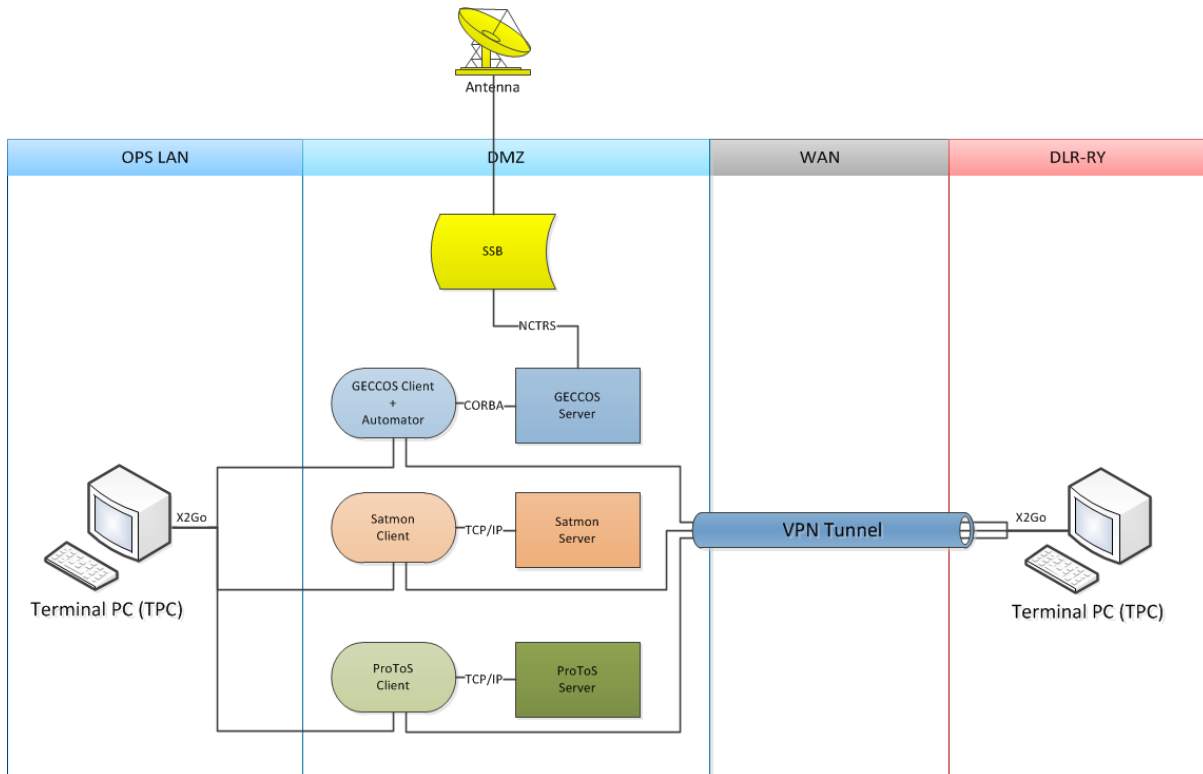


Fig. 4 Option 02: One command chain, clients in DMZ and remote connection to OPS and DLR-RY

IV. Consolidated System and Central Checkout System

“Security counts more than costs and effort”. This simple slogan summarizes the weighting of the arguments for and against the previously described design concepts. The decision was taken to implement option 01 for S2TEP-1, although the costs and effort for S/W and H/W integration and maintenance are significantly higher than for the other options. However, it is the most secure option. No forbidden connections over the network border between Ops-LAN and the DMZ are established. No possibility to affect the multi-mission environment from a third party or by DLR-RY is introduced. SSH connections are commonly seen as very secure, even more if only graphical information is transmitted. Therefore it is agreed that the design of option 02 and especially the remote connections between Ops-LAN and DLR-RY to DMZ will be tested and validated in order to gather experience with these connections outside the Ops-LAN. If these connections result to be robust, secure enough, and operationally reasonable, the design will be adapted to option 02, since this is the favored alternative. It was described previously that synchronization of data and information might be an issue for the designated design. Therefore the data to be synchronized needs to be assessed and defined by MCDS and the Mission Operations engineers.

The first design proposal is not an option to be considered, as long as the current network infrastructure is in place at GSOC. The network infrastructure is currently being modernized [8]. Once this new network infrastructure is available it will be possible to operate various missions with different requirements in terms of security levels in separate VLANs.

The CCS will be implemented according to the chosen design. It is accessible from the remote control center as well as from GSOC in the same manner as an external ground station. From the set-up (see Fig. 5) it is transparent for the operator in the control room if the S/C in orbit or an engineering model is currently monitored and controlled. Thus ground segment component tests, procedure validation, trainings and simulations can easily be supported before launch. Technically this is realized by connecting the control center SLE user (SSB) with the SLE provider (available at the CCS in Bremen) over WAN through a VPN tunnel.

The intensive use of MCDS components in the checkout system is an additional pre-validation of the software. Mission specific adaptations and configurations are already tested at the integration site and potential errors or problems thus detected early.

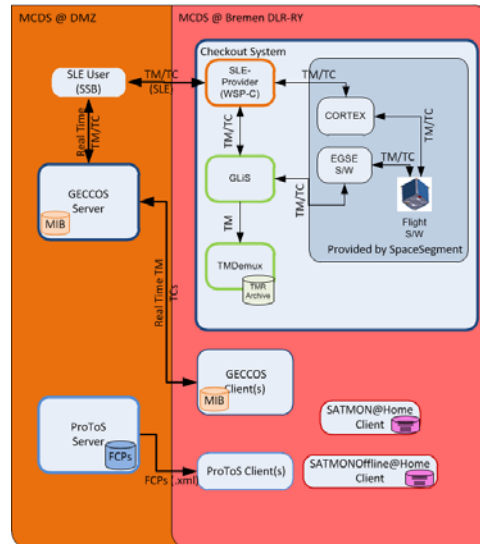


Fig. 5 Central Checkout System for S2TEP-1

V. Conclusion

Although S2TEP is a low cost mission, it necessitates challenging requirements for the ground segment, like the external commanding and a highly flexible mission control system. Eu:CROPIS, also a DLR-RY mission, follows, however, a more conservative mission operations design. Integrating into the current GSOC infrastructure the design that best meets the low-budget requirement of the S2TEP project, could arise security concerns. Although these concerns are not relevant to the project S2TEP itself, a security flaw within the S2TEP-1 ground system might take hazardous effects to the multi-mission environment and thereby to the other satellite missions at GSOC. As a consequence a more expensive design needs to be implemented.

GSOC has reacted on new requirements from customers and is going to change its network infrastructure in order to have the possibility to separate each satellite mission virtually within the multi-mission environment in future [8].

References

- [1] Dannemann, F., Jetzschmann, M.: "Technology-driven design of a scalable small satellite platform", The 45 Symposium 2016, Valetta, 2016
- [2] DLR - Institute of Space Systems - S2TEP, Retrieved from http://www.dlr.de/irs/en/desktopdefault.aspx/tabid-12525/21846_read-49985/
- [3] Zimmermann, S., Schulze, D., Stangl, C.: "Command Chain Automation", SpaceOps 2014 Conference, SpaceOps Conferences, AIAA 2017-1817
- [4] Beck, T., Schlag, L., Hamacher J. P.: "ProToS: Next Generation Procedure Tool Suite for Creation, Execution and Automation of Flight Control Procedures", SpaceOps 2016 Conference, AIAA 2016-2374
- [5] Stangl, C., Lotko, B., Braun, A., Geyer M.P., Oswald M.: "GECCOS - the new Monitoring and Control System at DLR-GSOC for Space Operations, based on SCOS-2000", SpaceOps 2014 Conference, SpaceOps Conferences, AIAA 2014-1602
- [6] Peat C., Hofmann H.: "SATMON -A Generic User Interface for Satellite Control", DGLR-2004-012
- [7] RHEA Group, White Paper: "MOIS - Manufacturing and Operations Information System", 2014, Retrieved from http://www.rheagroup.com/wp-content/uploads/2015/07/MOIS_White_paper.pdf
- [8] Hauke, A. & Geyer, M. P.: "Hosted Control Center – A concept for a flexible future satellite ground system", SpaceOps Workshop 2017, Moscow, 2017