Satellite Test Center (STC)

Collocated remote Spacecraft Testing
March 2017

Karel Kotarowski[1], Robert Traussnig[1], Joachim Stark[1]

[1]AIRBUS Defence and Space
Claude-Dornier-Str., 88090 Immenstaad
GERMANY
karel.kotarowski@airbus.com
robert.traussnig@airbus.com
joachim.stark@airbus.com

INTRODUCTION

The Satellite Test Center (STC) project is a R&D improvement initiative developed by Airbus Defence and Space at Friedrichshafen to improve the collocated remote satellite and payload testing.
Development of functional operation on large space projects is more and more shared between companies, countries and sites. The final integration and testing on spacecraft level requires a deep expertise and engagement of all parties to efficiently progress with functional tests in time and cost boundaries. AIRBUS Defence and Space developed a concept to facilitate a collocated remote operating team interconnected with a matured tool suite to cover diverse needs within the assembly integration and test phases of satellite missions, scientific exploration probes and payload or instrument components.
This approach benefits in a reduced need for travelling, improved balancing of human resources including the reduction of staff idle time on campaigns and efficient remote access to telemetry and scientific data.
Considering current security situation related to internet based connectivity, the STC concept mitigates computer based attack scenarios by implementing and elaborating state-of-the art point to point security solutions including a sophisticated active threat monitoring service.
The STC itself is a suite of tools, processes and documentation. It consists of hardware, software, documented processes and methods as well as advices, analyses and recommendations. Furthermore it is not a concluded project but a development still in progress, evolving, advancing and improving with each deployed implementation. This specific capability ensures technological adaptions and extensions to new developments and updated tools as they become available.
The STC also is flexible and modular. It can be adapted and tailored to each space mission’s specific needs and requirements without enforcing fixed methods and processes. This also means, the STC will adjust to an AIT plan yet being able to extend it with the STC specific benefits and added value.
The major concept behind the STC is to add the ability of separating the functional AIT testing and development team including engineering and experts from the actual hardware of the spacecraft. While in previous missions the whole team of operators, engineers, experts and managers had to be located close to the spacecraft itself in order to be able to command it, retrieve its telemetry, develop testing sequences and analyse and investigate problems, the STC obsoletes this requirement of proximity. Whether the separation is in the frame of different buildings on an Airbus site or different countries or even continents, the team of operators and experts always continues to work in the same fashion from the same place - usually located on the originating home site of the mission. While the spacecraft - or instrument payload - will travel to environmental testing campaigns abroad and eventually tread its final path to the launch site, the core personnel remains at the home site and performs all relevant activities from the STC control room. The savings due to the resulting travelling needs are significant and greatly contribute to a more effective and competitive budget allocation. So does also the general availability and reaction time of experts and specialists who are usually located at the home site and could contribute just in time remotely via the STC.

This paper will present the technology, the process complexity and security issues to be considered.

COMPARISON BETWEEN CLASSIC AND STC BASED AIT APPROACH

The classic AIT approach relies on a large project team (AIT, engineering, payload / instrument experts) which remains in close proximity to the spacecraft or payload most of the time. This includes tests and preparations at the home site (e.g. cleanroom facilities, check-out area), environmental test campaigns at a remote testing site (e.g. ESTEC, Toulouse, Cannes) and eventually during launch campaigns abroad (e.g. French Guyana, Russia, Kazakhstan).
The work areas required for debugging, preparing and validating of test sequences are bound to the PC terminals in the check-out area, physical presence in front of these workstations is mandatory in order to perform the necessary activities.
If payload telemetry is being generated, the scientist and expert teams need to travel to the spacecraft site in order to have access and visibility to their science telemetry and to be able to evaluate and validate it.

The STC based approach instead achieves independence between the spacecraft location and the test engineers by establishing remote connections to the processing systems used to control the spacecraft or instruments. The required computer terminals can be located in any suitable room without imposing the need to restrict working from the check-out area or a cleanroom.
Additionally a clear benefit arises from the opportunity to collaborate with other AIRBUS sites to absorb peak workload situations by contributing remote workforce via the STC infrastructure.
The scientist teams and payload experts are offered access to their payload processing computers also remotely, even allowing them to remain at their home sites and institutes while payload functional tests are being performed due to immediate and transparent access to all relevant telemetry and processing capabilities.
Eventually also customer representatives may benefit from the STC implementation if they establish a remote STC facility at their own premises to achieve the capability of joining milestone spacecraft tests remotely.
In summary, the STC based approach means that

- the STC facility located at an AIRBUS site maintains control, visibility and monitoring of the spacecraft
- the actual location of the hardware is not relevant to the STC operators
- the use cases involve spacecraft access at other AIRBUS sites, environmental testing facilities or launch sites
- the concept is universal, flexible and adaptable to diverse mission scenarios and project needs

USE CASES

Remote Testing of Spacecraft during environmental Campaigns

In this use case, the main operator team remains at their home site while the spacecraft travels to a testing site.
This results in a limited amount of required hardware / backup personnel on site during non-critical activities, like functional tests, preparation activities, dry runs, etc. Yet, the full visibility of all relevant telemetry, environmental parameters, Electrical Ground Support Equipment (EGSE) status or critical areas surrounding the spacecraft is available to the team remaining at the home site within the STC facility.
Additionally, the remote team has full commanding ability from the STC to perform all kinds of relevant functional tests remotely collaborating with the reduced local team ensuring optimal safety and reliability constraints.
The main control hardware including EGSE, Check-Out-Systems and Special Checkout Equipments (SCOEs) remains at the spacecraft in this scenario. Remote connections to these systems are performed only via remote desktop sessions and collaborative tools like WebEx for screen-sharing. This means, no telemetry or telecommands are acutally transferred, only user interactions which are then executed on the equipment at the spacecraft.
This working mode is comparable to the already used ESOC NDIU approach during IGST / SVT.

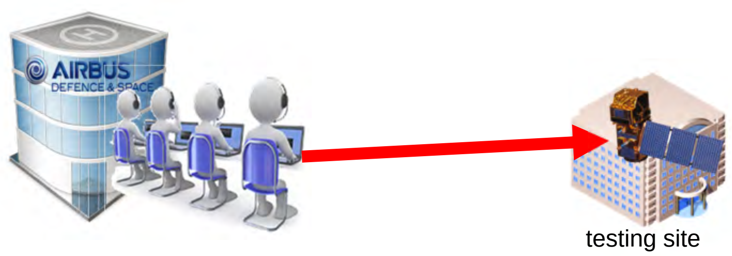

Fig.1. Remote Testing of Spacecraft during environmental campaigns

Remote Testing of Instruments during environmental campaigns

This use case includes an independent test of a single instrument or payload instead of the full commissioned spacecraft. The basic principle remains the same as for the spacecraft test. Also the main operator team remains at home and controls the instrument from the STC facility with full visibility of all relevant telemetry and commanding ability. At the instrument site, only a limited team is required to perform mechanical activities at the instrument.
This use case however also requires the transmission of the generated scientific instrument telemetry to the STC site for further post-processing and later evaluation. This is achieved with dedicated high bandwidth lines which ensure real time processing and analysis remotely by the experts. The local team which remains at the instrument has advanced communication options to stay in close touch with the remote operator team, e.g. to perform mechanical calibration settings or modify specific parameters directly at the instrument hardware.

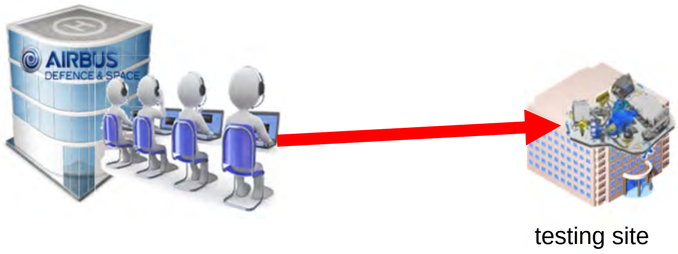

Fig.2. Remote Testing of Instruments during environmental campaigns

Remote Customer Participation at milestone tests

It has been understood that the customer has a high interest to take part during crucial milestone tests, even before environmental campaigns start. Test cases like major SVTs and ISTs including payloads and specific subsystems provide a good opportunity to evaluate the current performance and maturity of a spacecraft, especially when tests are prepared at engineering models for the flight hardware.
In this scenario, the customer receives a dedicated, so-called “STC light” installation to participate at specific pre-defined tests remotely. When ready, the STC facility grants the customer’s STC-light facility monitoring capabilities restricting any kind of control or direct access to spacecraft commanding options. This way, the customer does not have to travel to the spacecraft to participate at the relevant tests but instead may follow them with his own team remotely yet having full visibility of relevant telemetry, synoptic pictures or alphanumeric data displays on his demand. Based on the involved check-out-system and privileges, the customer may even retrieve historic data or arrange his own display set of windows and parameter lists independently from the STC operators and without affecting them at all.

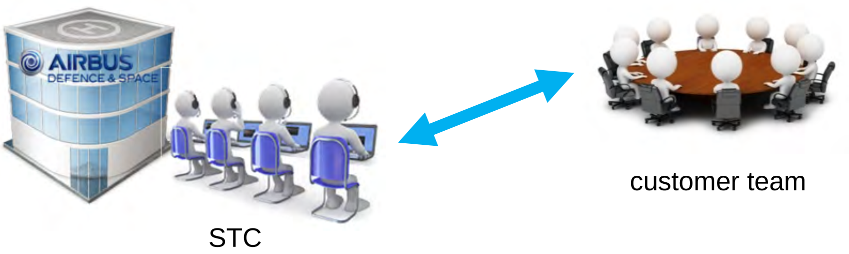

Fig.3. Remote Customer Participation at milestone tests

Scientific Data Retrieval and Analysis for Principal Investigators (PIs) and Instrument Cognizants

This is actually not an independent use case of the STC but instead a specific working mode in which external partners like instrument principal investigators are offered access to their own provided equipment (e.g. Instrument-EGSE) at the site of the spacecraft's current location.
In a check-out environment, generally two kind of EGSE is deployed: these who are required to operate the spacecraft or stimulate its sensors, like the Central Checkout System, Power SCOEs, TM/TC Equipment or Startracker Stimulators and EGSE, which is processing the telemetry generated by the spacecraft (usually coming from its payloads and instruments). This Instrument-EGSE is usually directly provided by the PIs and consists of Laptop or Desktop PCs. These computers run software to process, evaluate and validate the telemetry and provide an analysis of the proper functionality and comparison of expected results from the instruments. Operation, maintenance and support of this Instrument-EGSE are done by the PIs themselves which involves direct access to the related computers.
The STC is capable of providing secure and easy to use access to the Instrument-EGSE for external PIs over the public internet so the scientists could connect from their home sites to their equipment located at the spacecraft's current location and operate the analysis and processing tools remotely. This working mode reduces the travelling amount significantly and also is highly appreciated by the customer.

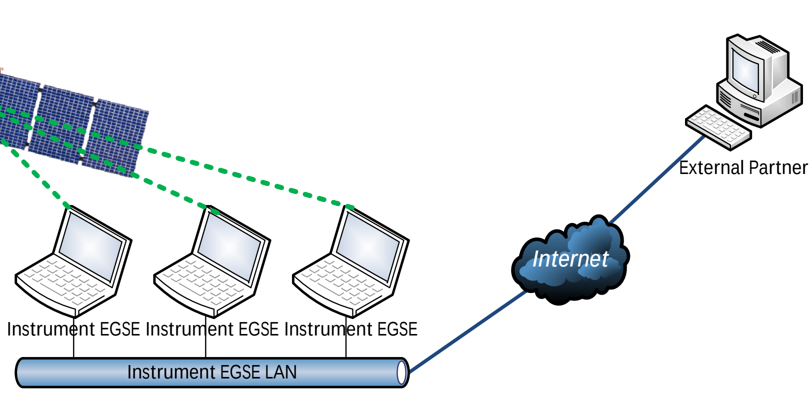

Fig.4. Scientific Data Retrieval and Analysis for Principal Investigators (PIs) and Instrument Cognizants

Remote flexible workforce contribution between AIRBUS sites

The STC infrastructure is not only useful for campaign support of spacecraft and instrument activities but also allows benefits and opportunities for flexible workforce management between AIRBUS sites to mitigate peak workload situations at specific sites. This facilitates new working modes, especially around the resource consuming test and debugging activities on EFM test benches. As the STC allows remote collaboration e.g. for test sequence preparation, debugging and execution, remote teams can be quickly assigned to these tasks without the need of physical relocation and changed working contracts due to migration needs. This working mode has been proven highly efficient, flexible and adequate as it can be quickly established on-demand and also does not impose any delays usually introduced by employment demands. As this working concept depends on already existing and available intersite networking infrastructure, the implementation effort is low and the time to productive availability is very short.

Fig.5. Remote flexible workforce contribution between AIRBUS sites

COMPLEXITY OF THE PROCESS IMPLEMENTATION

Complexity in the Technical Realisation

The implementation effort requires solving several technical challenges.
First of all, the foreseen networking solutions need to be defined with sufficient margin in order to cover the performance requirements wrt. bandwidth and latency.
Additionally the link security is a critical part to ensure a safe and reliable link protected from external and internal threats respecting the project knowledge and sensitivity of data. The live video links require compatibility with corporate videoconferencing standards to be accessible also from standard videoconferencing rooms.
With the introduction of thin clients at the workstations, a change of mind at the operators has to be considered as they need to incorporate a working mode where all data remains on virtualised servers and the client machines only provide keyboard, video and mouse accessibility. Complexity in the process also arises from accommodation and infrastructure requirements as the proper balance between comfort, effectiveness and security has to be considered.

Complexity in the Process Implementations

Besides the technical complexity also the processes add to the amount of challenges as several rules and laws have to be respected in order to prevent violation of existing laws and regulations.
These include national and European laws, company rules or site specific rules and labour regulations to be negotiated with the working councils, like the permission to use videoconferencing tools outside related video rooms).
Therefore the work process descriptions need to cover the applicable rules yet be efficient and compatible to the STC approach and furthermore applicable to other sites as well. Besides of this, a consequent paperless process is essential.

Complexity of inter-human behaviour and habits

An important aspect within the STC implementation is change management to be applied when employees who are used to common and ever-used processes have to adapt to a new and less well known process.
In many cases a general sceptic attitude towards remote operations needs to be addressed at different hierarchy levels during the implementation. Furthermore the confidence in a reliable and (fail-)safe, performant operation has to be established by gaining trust in the new tool by a good documentation and several performance and reliability tests.
Customer objectives as well as team objectives require consideration and need to be respected and balanced against each other, which may include the reduction of the overall cost base, increase of transparency towards the customer, raising and improving effectiveness of work and extending the flexibility to quickly react to unexpected situations.
Eventually, opportunities to gain savings need to be addressed, evaluated, defined and chased as one of the main benefits is the improved cost effectiveness resulting from the STC approach.

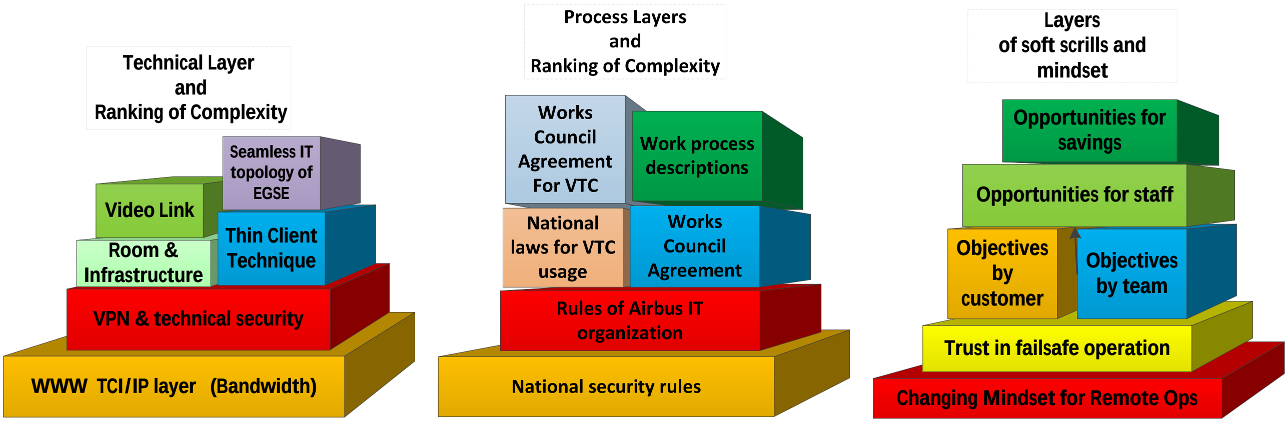

Fig.6. Layers of Complexity

STC DATA LINKS AND CONNECTIVITY

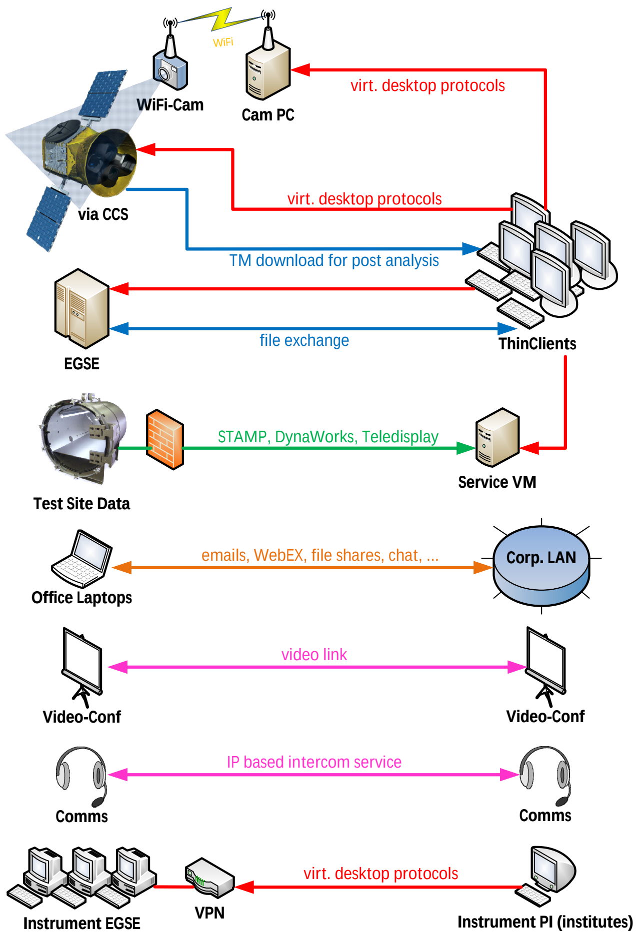

Fig.7. Data Links used by the STC

Wifi-Cam

Provides real-time video of the S/C or parts of it. Can be used by engineers during NCR investigations as a carry-on item to point on locations of interest. Could also be used for EGSE related investigations. A technician can highlight any item that needs to be observed or verified remotely.

The WiFi camera is connected by secure (WPA2-AES-personal) WiFi to a management PC. This PC shows the live camera image on its desktop within a dedicated application. Remote clients can connect via virtual desktop protocols to this PC. So the camera data are not distributed directly but instead, remote sessions to the desktop of the management PC allow to see the live camera image.

S/C access via CCS

Remote engineers can access the CCS connected to the S/C by virtual desktop links. The idea behind the approach is to allow remote engineers to see exactly the same applications and controls as if they would be present on-site. While the HW and SW remains physically on S/C site, the remote engineers participate via the virtual desktop links as if they would be locally present. This includes S/C control as monitoring and access to all relevant functionality and data. The TM furthermore can be downloaded remotely to allow post-processing and further analysis independent of the on-going test on S/C site. A dedicated setup for customers allows them to participate in tests viewing relevant S/C TM streamlined to the customer's needs. This can be considered as an excerpt of the test data providing the customer a comprehensive view of relevant data and TM.

EGSE access

The EGSE on S/C site can be accessed via virtual desktop links. This allows EGSE managers to verify and optimize the EGSE functionality re-motely as well as to include patches and fixes on the fly. Test engineers can keep track of EGSE status and function remotely and perform regular activities.

Test Site Data

Test sites provide critical data as temperatures, pressures, solar flux, mechanical status of S/C adapters, etc. to their customers. This data can be accessed remotely and evaluated by the test engineers.

Office Laptops
Engineers on campaign require access to corporate applications as email, network shares, e.g. remotely. Secured VPN tunnels allow them to connect to the corporate LAN in remote offices without inconvenient login procedures. The corporate laptop device is a key element to access data on campaign and stays connected to the corporate environment at all time.

Video Conferencing
A dedicated video conferencing system between the remote test site and the STC lab allows distributed teams to discuss and consolidate on AIT topics face-to-face. This feature can be used for daily meetings as well as phase change meetings to provide real time status of tests.

Comms Systems
All involved personnel is equipped with portable headsets. Each member can directly talk with each other over secured voice links. Group communication is also possible. Team members can easily setup conferences or talk to other members via the voice link.

Instrument EGSE
Instrument PIs can access their EGSE located on S/C site remotely by secure VPN access from their home offices. While the I-EGSE is provided and maintained solely by the PIs, the STC infrastructure provides them access to their systems all over the world.

HERITAGE AND EXPERIENCE FROM PREVIOUS PROJECTS

The first project to implement an early prototype was BepiColombo, where the STC was used to monitor tests running at the ProtoFlightModel first in Turin and later at ESTEC from the Engineering Test Bench in Friedrichshafen. The STC also provided infrastructure for data exchange between both benches and introduced the concept of remote access for instrument PIs to their Instrument EGSE. The experience from the BepiColombo prototype showed the need and requirement for enhanced and comprehensive collaborative tools besides the possibility of a remote spacecraft access.

Sentinel-2 followed with the first representative implementation of a dedicated STC facility with live videoconferencing and a thin client based access approach to a remote server. For the first time, the STC was used to support and monitor the spacecraft activities during an environmental test campaign with two distributed teams collaborating with each other via the STC tools. The experience from Sentinel-2 showed that a performant, reliable and secure networking layout and infrastructure are crucial for robust and effective STC operation.

Grace Follow-On (GFO) was the first project to support a productive and complex STC working mode including live remote commanding of two GFO spacecraft in parallel from a dedicated STC facility which also completely replaced the classic check-out area. The GFO STC furthermore introduced live images from the clean rooms showing the spacecraft under test to increase human and hardware safety by monitoring mechanical and electrical activities at the two spacecraft and also having warning lights (RF, bus power) always visible in the transmitted pictures. The experience from GFO showed that live images from the spacecraft increase the safety and offer better overview to remote operators providing them the current view of the hardware. Additionally it has been observed that the location of the STC facility on the project floor (close to the engineering team and other project colleagues) greatly improves the team communication and ease of access to relevant data assisting the change of mind by using the STC tool.

The STC has also been implemented for Sentinel-5P to establish cooperation between the AIRBUS sites at Stevenage and Toulouse and furthermore is in development for the SOLO campaign as well as Metop-SG, JUICE, Sentinel-5 and Sentinel-6. Further projects will also implement the STC as it clearly proved an increase of efficiency and economy.

SECURITY CONCEPT

The STC security concept was developed in the frame of an AIRBUS Product Security R&D project, in close cooperation with AIRBUS Cybersecurity.

A risk analysis based on the ISO/IEC 27005 Information Security Risk Management standard has shown three major cyber attack vectors to be considered:

1. Man-in-the-middle attack performed on the VPN link between the STC and the remote site(s)
2. Malware injection into the endpoints (both STC and remote sites)
3. Exfiltration and loss of intellectual property and/or sensitive data

To mitigate these risks, the security concept has been based on state-of-the-art technology and services made in Europe.

The AIRBUS-developed high-performance **STORMSHIELD Network Security (SNS)** network appliance has been selected to protect the Internet-link between the STC and the remote sites.

STORMSHIELD is a next-generation Firewall and Unified Thread Management (UTM) appliance with the following characteristics:

- Next Generation Firewall/UTM developed in Europe
- Advanced Security Qualification Engine (ASQ) as an integrative and intelligent combination of functions
- Low false-positive rate, high-performance, broad application support
- Integrated detection and mitigation of vulnerabilities in IT infrastructures
- VPN (IPSec, SSL)
- CC evaluation and certification
- Throughput up to 130 GBit/s, suitable for secure high-bandwidth scientific payload data transfer

Fig.8. STORMSHIELD features

The STORMSHIELD performs a full chain of automated functions, ranging from protocol analysis, behaviour-based analysis and anomaly detection, content filtering / IDS / IPS, detection and mitigation of vulnerabilities, Network Address Translation, VPN and routing.

Fig.9. Automated Function Chain

The main axis of defence against the defined cyber risks is compulsive security monitoring and immediate reaction, provided by the three **AIRBUS Cyber Defence Centers** throughout Europe.

- Security monitoring includes the VPN links between STC and remote sites
- Non-intrusive monitoring of relevant Endpoints (e.g. SCOE, CCS)
- Immediate notification of STC team in case of DDoS (Distributed Denial of Service) attacks, link termination and smooth handover of operations to remote team
- All cyber experts at one place for fast detection, analysis and incident response
- Cyber protection measures (prevention) are continuously updated in order to be able to meet the latest threats
- Using a combination of voluminous cyber threat intelligence, advanced analysis methods, own tools as well as real-time monitoring for fast detection

Fig.10. AIRBUS Cyber Defence Center Overview