18th International Conference on Space Operations, Montreal, Canada, 26 - 30 May 2025.

SpaceOps-2025, ID # 554

OPERATIONS PREPARATION AND EXECUTION IN HIGH SECURE ENVIRONMENTS

Dr. Alan Moorhouse*[a], Markus Banholzer[b], Leander Wichel[b], Laura Taprogge[b] , Stephan Bechtold[b]

[a] OHB Digital Connect, alan.moorhouse@ohb.de +49-421-2020-9558
[b] OHB Digital Connect, Lise-Meitner-Str. 2, 28359 Bremen, Germany
* Corresponding Author

Abstract

This paper will describe the experience, challenges, and counter measures taken from several missions, that cannot be declared here, both prepared and executed within secure environments in a generic manner. The missions are characterised by the necessity by a high level of data, system and personal security which creates a number of issues for reasonably costed Operations;

Team Building and Maintenance are strongly affected by needs for clearance with timescales up to a year or more for new Team members to be able to start training or working on the project. Prior to launch this aspect leads to delays, during operations though can be critical.

Communication is restricted especially exchanges with open environments (suppliers, experts, telephones, mobile data devices including Laptops and Telephones etc.) and strong need to know principles. At a simple level company Networks, or any external like Internet, may not be available on site.

Data and Software exchange: It is not practical that all are fully developed or tested in a secure environment, this means measures for controlled exchanges are required, even simple things like rollout of Operational Products are restrained.

Hardening systems imply periods of absolutely no change, or even use over several months.

Security logging and personal legal responsibility implies that some tasks cannot only be executed locally, and that Engineering staff are often occupied with supervision of suppliers instead of Engineering.

Despite the above constraints, which are contrary to efficient and even safe Operations, there are methods to manage them without inflating the Operations Teams or costs which this paper will explore.

This paper is not written by security experts rather Operations and Ground segment Architects and Engineers who have to deal with the security restrictions where "resistance is futile"

Keywords: Preparation, Execution, Secure, Teaming

Nomenclature
None

Acronyms/Abbreviations
None

1. Introduction

This paper will report on the challenges in preparing for and executing Operations in highly secure environments, these are twofold both Technical and Personal related and fundamentally restrict the flow of information.

Missions with high levels of security clearance are thus characterised by;

1. Restricted Personal requiring security clearances from official bodies
    a. Individuals can become long lead items before being allowed to start training.
    b. Replacement and coping with unexpected absences is challenging

2. Restricted buildings, sperrzone
    a. Enhanced access control
    b. Security checkpoints
    c. Security controls
3. Restricted data
    a. Definition, and formal acceptance, of exceptions
    b. Control and reduction of all red/black secret to non-secret interfaces, typically including checks on information data types and content as standard.
    c. Clear definition of all operational data to be exchanged with unclassified entities, including orbital data!
4. Restricted Hardware movements
    a. Certification, accreditation, logistical movements
    b. Well maintained inventories
5. Restricted mobility, no use even carrying of;
    a. Laptops,
    b. Mobile devices (smartphones, etc.)
        i. Imagine the freedom of 8 hours `offline´
    c. Media devices and media

Along the motto once in, never out and if you let it out ensure no information is transmitted. Of course this motto cannot apply to people, hence the security clearances to ensure that "Secret" information is never unknowing released into the open.

2. Team and Personal

In terms of Operations preparation and execution resilience is important matter which is typically ensured by having a larger pool of trained experts available. In secure environments this pool is harder to build as some employees do not agree to (in Germany this is an employee decision), or will not be able to, obtain clearance.

In a more open Operations world appropriately qualified staff would be identified or hired at need, a process itself that can take weeks or months, and be immediately able to start working or training on the mission at hand. For Team building and ramp up in secure environments there is an extra layer that the new Team member requires clearance prior to being able to start any activities including access to reading material.

This clearance is typically the responsibility of governmental bodies and the requesting body has no influence on the timescale or result AND can only be requested once the concerned person is employed. After this then internal processes need to be followed

How does this impact the Operations preparation?;

1. Long lead time for employment Recruitment time + X Months,
    a. Where X > 3 Months and non predictable.
2. Real Risk that an available or employed person will not be cleared.
3. Implies
    a. Early Planning
    b. Resilience in the form of more than one potential resource acting as deputy/replacement
    c. Security to be addressed up front

The impacts are more extreme during late phases prior to Launch or during execution as unexpected unavailability or employees (via leaving the company, illness, etc.) cannot be compensated without extra mitigation measures.

What mitigations can be considered within Operations Execution;

a. Means an extra Team member per role.
b. Trained and ready to go
c. Priority agreements with other projects

The whole Team needs to be considered here, including specialised communications, hardware, software teams as well as those in second line support roles including the Satellite manufacturer Team.

In a typical project the whole team is composed of contributors from many departments and even companies, not all of which require clearance for their specialised contribution. Here an early buy in of the responsible managers is required to give a priority to clearance in advance and a continual reminder. Exceptions to security rules are by experience almost impossible to achieve. Extreme late measures include adapting the Sequence of Activities due resource constraints.

2. Restricted buildings

Working in restricted environments present an administrative and personal challenge. Typically, this may involve;

- a tighter access control than in "normal" office environments down to the individual level
- extra physical access, i.e keys
- deposit of proof of Identity (i.e. passport)
- Accompaniment of non "project" visitors or support staff
- Cleared suppliers (including Sanitary Management)

There is with all of the above an additional effort involved not only from those involved with access administration but also from on-site employees, i.e. Operator Staff. It is quite common that personal who are both security and project cleared need to spend time shadowing non project cleared ranging from customer, administrative staff (i.e. Human Resources, Health and Safety, Management), through to suppliers. This can reduce the available work hours available to Operations on average by up to 20%, depending upon the location and scope of work, i.e. it is easier to manage in the larger organisational home base than in a dedicated facility. Further in dedicated facilities, or even those of the customer it means that a local security officer role is required and needs to be considered even in the recruiting process.

3. Restricted Data

In general the Red Black Architecture refers to a segregation of areas that hold or carry `classified` plaintext (readable) information [RED] to those areas where the "classified" information is no longer readable (Encrypted) [BLACK]. This is a terminology and concept introduced in security engineering where red is internal and black the more public area.

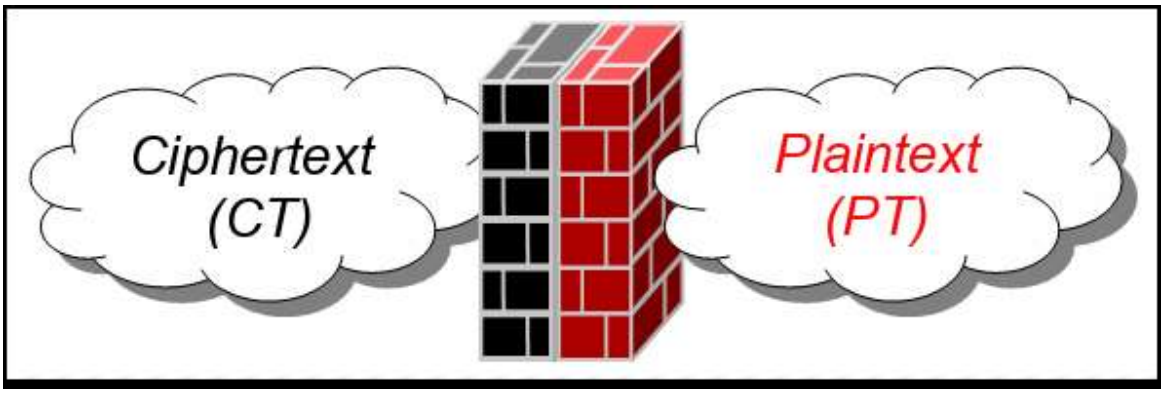

Fig. 1. Red Black Concept. Courtesy Wikipedia [1]

Thus the Data in the Red area is freely accessible, which is why great care is taken as to who can gain access to the red area. Probably the biggest challenge with working in secure environments is the data information flows which are by definition secure but facing the real world.

This implies that no information is allowed to leave the secure Red area unprotected (without for example encryption). Exceptions are pre-defined, agreed and controlled.

a. Pre-defined in dedicated control documents describing the security level of each and every piece of information
b. Agreed in the sense that the above is an official document of the customer.
c. Controlled in that the listing cannot be simply changed (could affect the accreditation) and that the electronic transfer is checked not only according to data type but also content (i.e. Ground Station ID in a scheduling request)

Fundamentally every person involved in a transfer of data from Red to Black is personally responsible for the security, in Germany under threat of criminal charges.

Further for electronic processes with "automatic" distribution, ie. Scheduling, Orbit Data, and so on the interface typically needs to be controlled to check that the data is indeed allowed. This makes format and/or content changes not easily modifiable – for example it may take months to change a parameter value if Gateways need to be updated.

4. Restricted Hardware

In general, the Architecture, Hardware and Software selection as well as deployment is something that takes place during the design and implementation phases of a project and not during the operations (exception is regeneration of Hardware/systems beyond their shelf life, which this paper will not discuss)

However, even during the realisation phase the security issues may affect Operation preparation, in the sense one works in a restricted environment AND that these systems require certification.

As certification takes place at system level some functions or even the complete system can become unusable during the certification process as it is locked for that purpose. Worst scenario is a control centre which can no longer be used for several weeks which conflicts with large events like Rehearsals. Of course one plans upfront to avoid such conflicts, but as always in OPS it is wise to have a back up plan just in case.

Moving devices into the secure environment undergoes a similar process of security considerations during design and implementation but are isolated to the function that the device will provide in terms of outages and are thus easier to manage.

Moving devices out of the secure environment is in the reverse also not straight forward as it must be ensured that no information leaks out into the open… This results in a tightly controlled and managed inventory list in order to know where everything is, for discarded components over several years of operation this can cause security headaches if the serial numbers do not match in the records.

5. Restricted Mobility

Data mobility is these days essential but also a weak point in any secure consideration. What brings a Red Black Architectures when even the cheapest (and small) smartphone can record unknowingly Gigabytes of data.

As such typically no mobile storage devices are allowed in secure areas including but not limited to USB sticks, DVDs/CDs, storage media, phones, smartphones, smartwatches, tablets, Notebooks, and so on. All such items need to be stowed away before entering the controlled red zones.

On the one side this makes data transfer into the secure environment laborious, for example special mechanisms are required for a Software release via physical medium and several authorisation/Authentication checks.

On the other side connecting with colleagues in the Zone is typically only possible via fixed phone lines, other means are prohibited except for agreed on all sides, secure communication channels. These channels are typically not available to support and administrative functions creating accessibility overheads.

From the other [red] side is a life from days gone by without mobile devices or smartphones, or readily available Network data. A typical shift is 8 hours which is conducted quasi offline – even some younger colleagues find this attractive but is not an option for many Employees!

6. Conclusions

Operations are of course possible within secure environments although as opposed to more open ones the resource planning and data exchanges are somewhat hampered which increase running cost and durations of even simple tasks. Further the demands and restrictions on individuals are quite extreme and do not fit the lifestyle of many which hampers Team build up and maintenance.

Acknowledgements

The authors would like to thank all colleagues who have worked in and overcome the challenges described in this paper

References

[1] CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=30107311, (accessed 14.05.25).
Reference to a conference/congress paper:
[2]