Satellite Test Center (STC)

ESA SESP Conference 2017

DEFENCE AND SPACE

Karel Kotarowski / Robert Traussnig
29 March 2017

AIRBUS

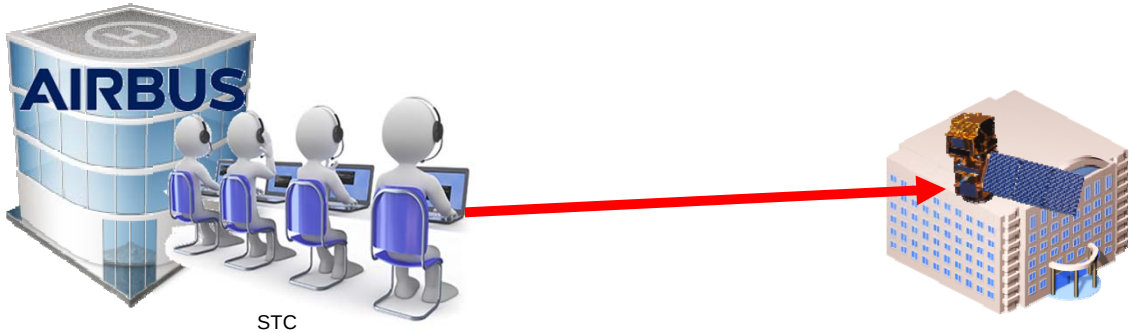
Agenda - The Satellite Test Center (STC)

- STC use cases
- technical setup
- data links and connectivity
- implementation roadmap
- challenges during implementation

- Cyber attack vectors
- AIRBUS Defence and Space Security Framework
- STC security concept

AIRBUS

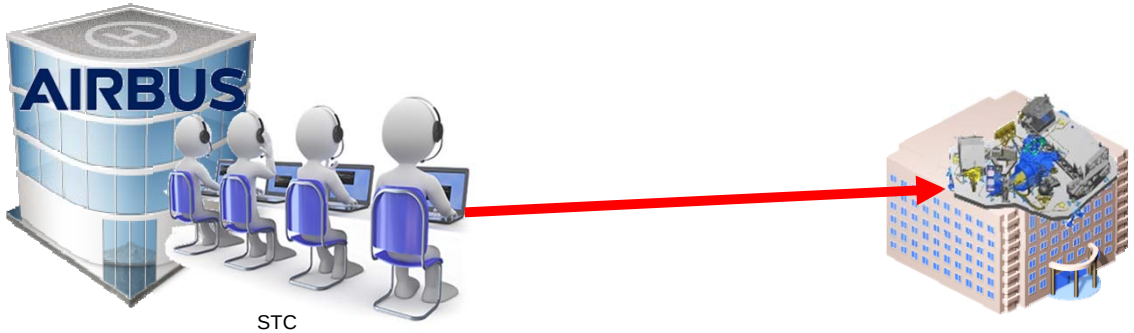
Use Case: remote testing of **spacecraft**



- the main operator team remains at home site while the spacecraft travels to a testing site
- only a limited hardware / backup team travels with the spacecraft
- full visibility of all relevant telemetry + environmental parameters at the STC
- full commanding ability to perform all relevant functional tests remotely
- the main control hardware (EGSE, Check-Out-System, SCOEs) remain at the spacecraft
- remote connections via remote desktop protocols are used for access
- collaboration tools (videoconferencing, WebEx, etc.) support the cooperative working mode
- this is basically an advanced model of the already in-use ESOC NDIU access for IGSTs / SVTs

AIRBUS

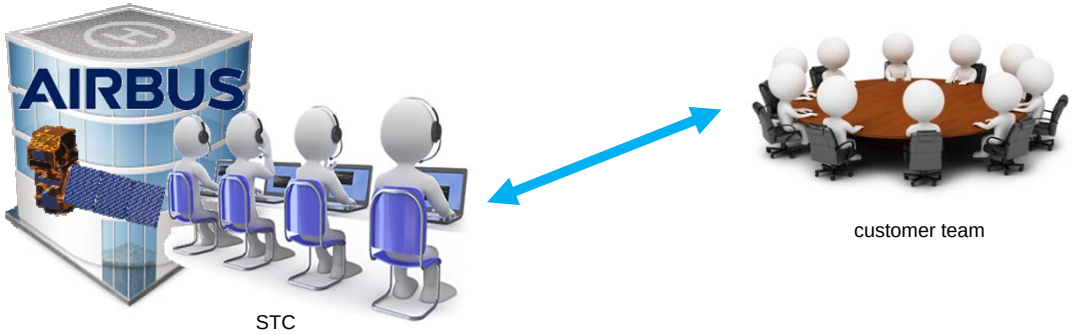
Use Case: remote testing of **instruments**



- the main operator team remains at home site while the instrument travels to a testing site
- the instrument is left autonomous, only emergency engineers remain for contingency procedures
- full visibility of all relevant telemetry + environmental parameters at the STC
- full commanding ability to perform all relevant functional tests remotely
- the main control hardware (EGSE, Check-Out-System, SCOEs) remain at the instrument
- remote connections via remote desktop protocols are used for access
- scientific data from the instrument can be transferred in real time to processing servers on home site via dedicated high-bandwidth lines

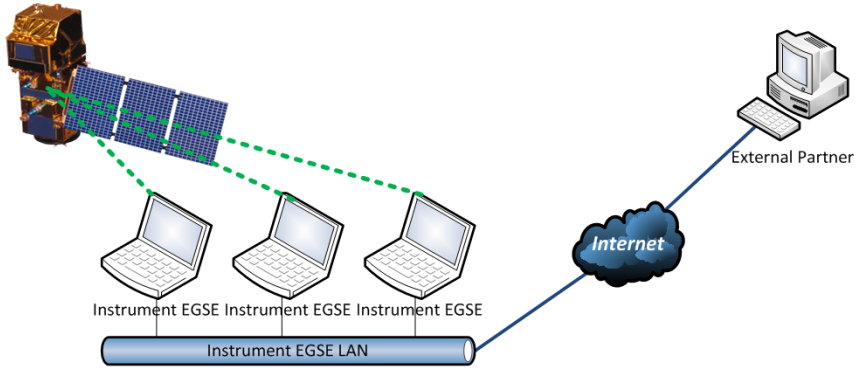
AIRBUS

Use Case: **customer** participation at milestone tests



- the customer receives a dedicated STC-light installation to participate at specific tests
- access for the customer with monitoring capabilities is enabled from the STC
- observability of all relevant telemetry / synoptics at the customer premises
- results and findings are available at customer level immediately after the test based on the acquired telemetry
- the customer can select interesting telemetry, browse retrieved data or view relevant synoptics independently from the main test operator console

Use Case: scientific data retrieval + analysis for **PIs**



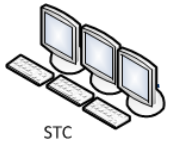
- science teams of the instrument / payload suppliers can access their own equipment located at the spacecraft's current location
- the science data is transmitted and stored on the computers located at the spacecraft site (EGSE / SCOE room)
- external instrument / payload partners get specific and secure access to these computers which they provided to the project
- instrument / payload supplier teams can work independently from their home sites, esp. without specific office hours requirements

AIRBUS

Use Case: remote **flexible workforce contribution** between AIRBUS sites

- peak workload situations at one AIRBUS site can be flexibly balanced by remote workforce contribution by other sites
- employees work remotely via a STC instance on their home site, no need to relocate personnel or change working contracts due to migration
- quick and efficient working mode, no need to wait for new employments and no need to lay off personnel if the workload normalizes again
- secure AIRBUS intersite-networks can be used for that approach, infrastructure is already in place

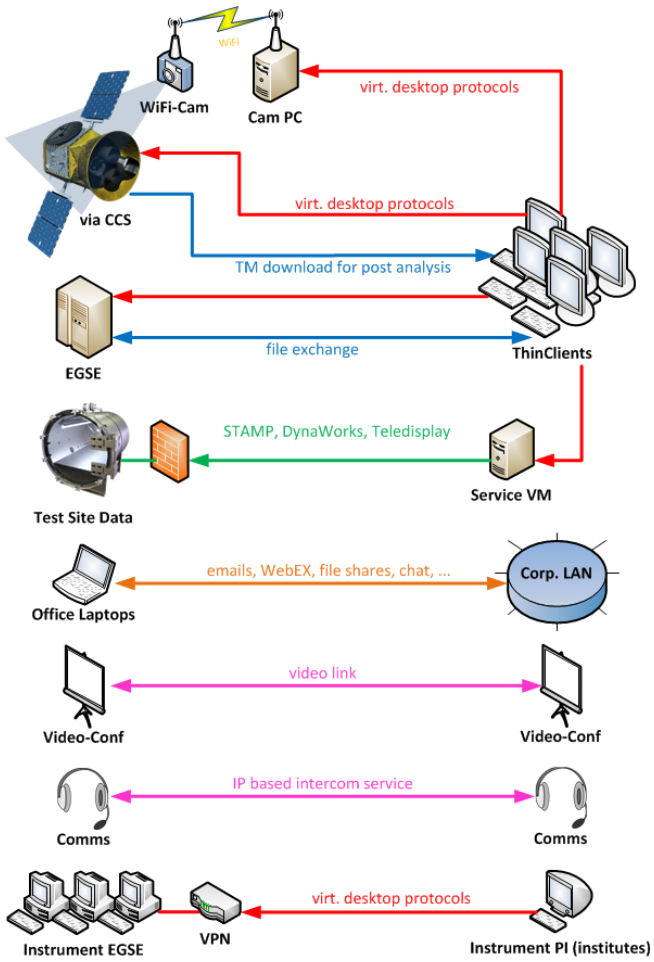
Technical setup



- secure remote desktop connection to the Central Checkout System
- the virtual display (desktop) of the CCS is transmitted remotely but no actual TC / TM data
- local operators can take over the spacecraft if necessary to maintain safety of hardware
- all critical infrastructure necessary to operate the spacecraft remains with it - same safety level as with the classic AIT approach

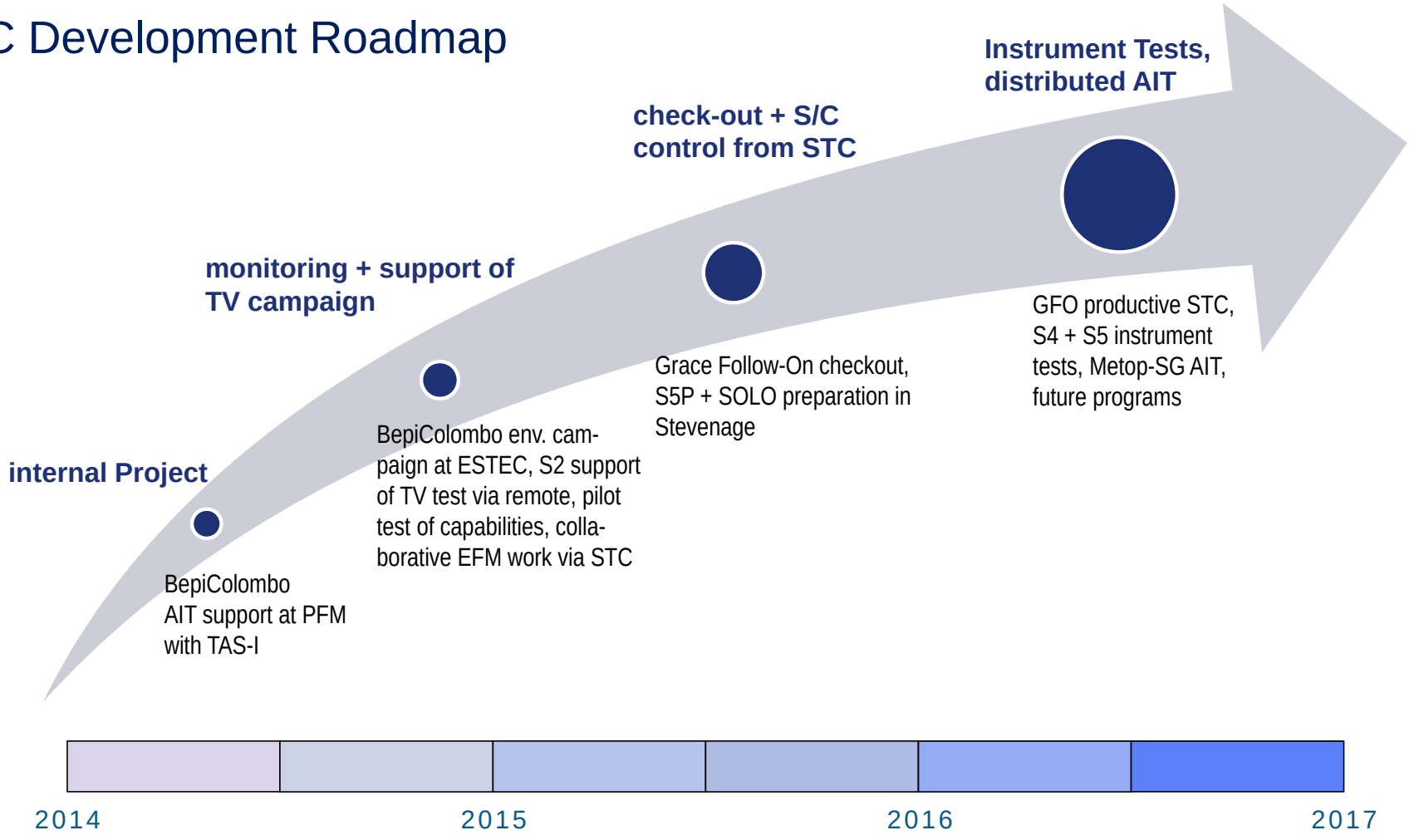
STC connectivity

- Live images of the S/C are transmitted via wired or WiFi-cams to a cam PC which is connected by RDP to the STC
- all CCS links are established via remote desktop sessions
- TM can be downloaded for post processing from the S/C
- TV facility status data (temp., pressure, lighting, etc.) are available at the STC in realtime
- office laptops of AIRBUS personnel have full corporate access inside the STC and remotely on campaign (e.g. Email, WebEx, file shares, internet)
- remote and STC teams communicate via permanent high-resolution videoconferencing systems
- clean-room communication (incl. ISO 5) via special intercom headsets with Matrix-VOIP
- specially secured VPN tunnel for PI access to their payload instrument EGSE



AIRBUS

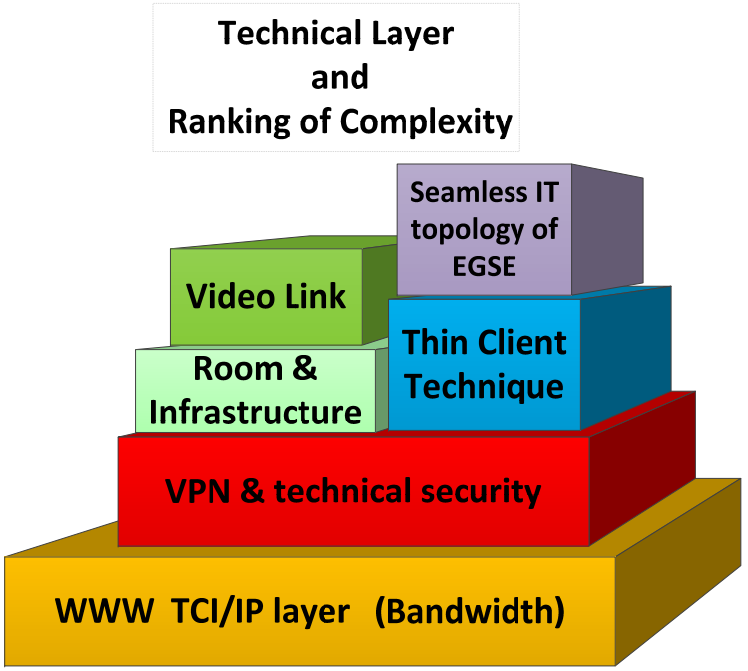
STC Development Roadmap



AIRBUS

Complexity and challenges in the technical realisation

- **networking solutions** need to be foreseen to cover the performance (bandwidth, latency) requirements including reliability and redundancy
- **strong security** is essential to protect the service from malicious access and attacks and ensure sufficient protection to the knowledge and sensitivity of data
- live **video links** require compatibility with corporate videoconferencing standards
- the **Thin Client working mode** includes a change of work habits where all data remains on virtual servers and clients only are used to provide KVM accessibility
- **accommodation and infrastructure** need to cover the demands for comfort, effectiveness and security
- the **EGSE topology** need to be compatible with a remote operation approach and provide relevant interfaces

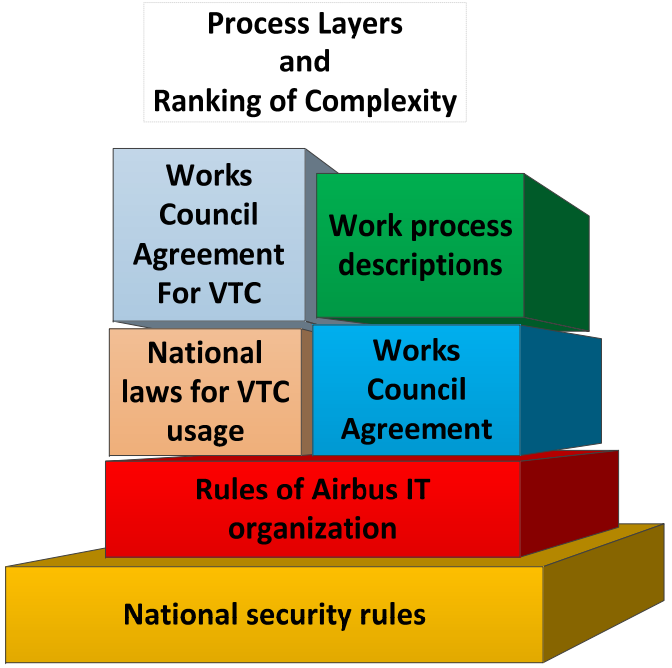


AIRBUS

Complexity and challenges in the process implementations

- several **rules and regulations** are to be respected
  - national or European laws
  - company rules or site specific rules
  - labor regulations negotiated with working councils (including permit to use videoconferencing outside related video rooms)

- **work process descriptions** need to cover the applicable rules yet be efficient and compatible to the STC approach and furthermore applicable for other sites as well



AIRBUS

Complexity and challenges with mindsets and change-management

- **general skeptic attitude** towards remote operations needs to be addressed at different hierarchy levels
- confidence in a **reliable, (fail-)safe and performant operation** needs to be established
- **customer objectives and team objectives** need to be respected and balanced against each other
  - reducing the cost base
  - increasing transparency
  - raising effectiveness
  - improving flexibility
- opportunities to gain **savings** need to be addressed, evaluated, defined and chased

AIRBUS

STC pilot project: Sentinel-2

The first full-featured STC prototype

Remote operation with one spacecraft in

- IABG Muc. (environmental test)
- Kourou (launch prep)

The first milestone to achieve the distributed AIT scenario.

AIRBUS

STC productive implementation: GRACE Follow-On

The first productive STC implementation

Remote operation with two spacecraft in parallel.

- IABG Muc. (environmental test) currently

Later 2017 support of the launch campaign in Vandenberg / USA is foreseen.

AIRBUS

Cyber Security considerations

ensuring safety, security and mitigation of risks

AIRBUS

A few examples of how real cyber attacks are:

1982

Alleged **sabotage** of the Soviet Urengoy-Surgut-Chelyabinsk natural gas pipeline by the CIA.
How : Trojan horse injected via the Russian supply chain.
Consequence : Explosion of the pipeline.

2009

Operation Socialist: infiltration of Belgacom by NSA/GCHQ. Target : European cellphone comms.
How : targeted attack (engineers), internet traffic redirection, APT. Detected only in 2012/2013.
Consequence : Spying of European cellphone communications using Belgacom network.

2010

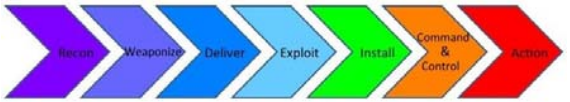
Operation Olympic Games / Stuxnet : attack on Iranian nuclear program (centrifuges used for uranium enrichment)
How : targeted attack (0 day), APT crafted specially for SCADA systems used in Natanz..
Consequence : estimated delay 5+ years to Iranian nuclear program. Origin : USA/Israel

2012

Nortel attack : Industrial espionage over a 12 year period (2000 – 2012)
How : password stolen from executives, rootkit, covert channels (encrypted data exfiltrated to China)
Consequence : espionage of top execs, R&T, finance, business plans. Direct contributor to company collapse

2013

"Target" attack : Payment information theft (point of sale)
How : via a subcontractor network (HVAC) connected to Target network
Consequence : Data from 70M credit/debitcards stolen



2014

Dragonfly/Havex : Industrial espionage on energy sector / pharmaceutical sector
How : waterhole attack / subco internet sites compromised (3 ICS vendors) to offer trojanized software.
Consequence : Targets critical Industrial Control Systems – Alleged origin : Russia – Target : Europe/US

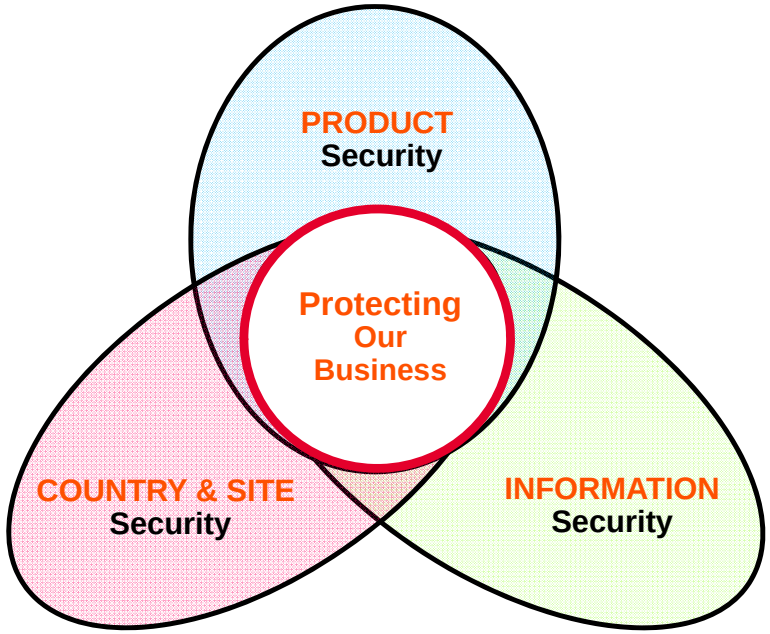
2014

German steel mill (BSI report 2014) : Manipulation of Industrial Control Systems
How : spear phishing ➔ corporate network ➔ production network
Consequence : Physical damage to the steel mill ("massive destruction")

2015

Equation group : espionage (allegedly developed by the same team that created Stuxnet)
How : attack via web exploits, USB, CD-ROM (conference proceedings)
Consequence : Exploit hides in hard drives firmware (impact 12 different vendors)

Airbus Defence and Space Security Framework



AIRBUS

Definition

PRODUCT SECURITY

Addresses the protection against **cyber threat** for the “products” we sell throughout their entire lifecycle, as well as ensuring all security requirements for the product’s **operational context** are appropriately specified and addressed.

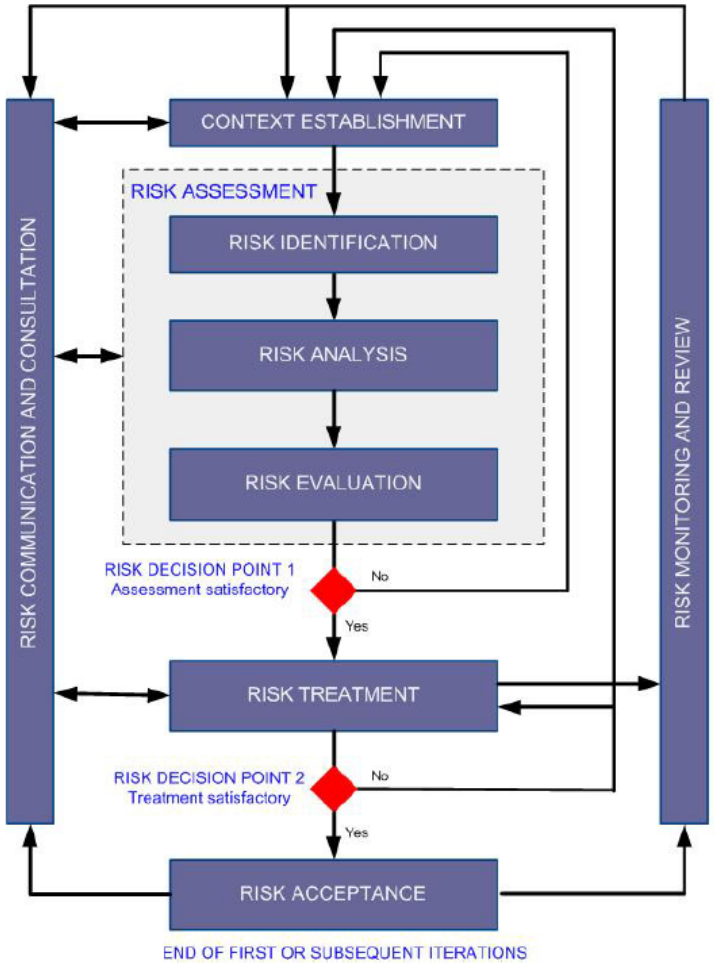
“PRODUCT” in the context of the Product Security initiative is:

Anything Airbus provides to a customer (internal or external) in any combination of:

- Tangible physical product (including but not limited to: component, LRI, platform, system, building, test equipment, spare parts, supplied COTS & MOTS, ….)
- Software/Firmware (including but not limited to: applications, updates, patches, configuration data, electronic service guides…)
- Managed Services (including but not limited to, NOC and SOC services, data services e.g. GEO Int, support centres, …)
- Documentation (user guides, instruction manuals, maintenance instructions…)

STC Risk Assessment ISO/IEC 27005

- Risk assessment based on the ISO/IEC 27005 Information Security Risk Management standard
- Three major cyber attack vectors to be considered:
  - Man-in-the-middle attack performed on the VPN link between the STC and the remote site(s)
  - Malware injection into the endpoints (both STC and remote sites)
  - Exfiltration and loss of intellectual property and/or sensitive data
- Risk Treatment / Security Concept defined, together with our collegues from Airbus CyberSecurity.



AIRBUS

STC Security Concept – Link Protection with Stormshield

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 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-bandwith scientific payload data transfer from remote site

AIRBUS

STC Security Concept – Endpoint Protection by Airbus Cyber Defence Centres

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

- Security monitoring includes the VPN links between STC & remote sites
- Non-intrusive monitoring of relevant Endpoints (eg. 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

Karel Kotarowski

Airbus Defence and Space

88039 Friedrichshafen
T: +49 7545 8 3939
E: karel.kotarowski@airbus.com

Robert Traussnig

Airbus Defence and Space

88039 Friedrichshafen
T: +49 7545 8 5615
E: robert.traussnig@airbus.com

Daniel Scheerer

Airbus CyberSecurity

82024 Taufkirchen
T: +49 89 3179 4957
E: daniel.scheerer@airbus.com

Thank you

AIRBUS