iABG

CHRISTIAN CRETER | CONSTANTIN SCHLACHETZKI | IABG DIGITAL ASSURANCE

ADVANCING CYBERSECURITY ACROSS DOMAINS

IN SUPPORT OF MILITARY, HOMELAND SECURITY FORCES & CRITICAL INFRASTRUCTURE PROTECTION

November 11, 2020 (Code 2020)

AGENDA

IABG – A leading European technology enterprise

Core competencies of analysis, simulation & testing as well as plant operation (safety & security)

IABG

- **1961** Company foundation as part of the German government
- **1993** Privatisation
- **1999** Satellite Teleport
- **2006** New defence & security simulation and test centre
- **2017** New simulation center for Cyber Security and innovative solutions based on Artificial Intelligence
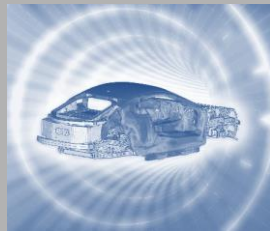- **2019** Groundbreaking for Competence Centre Optics (CCO)

87,4 %	**12,6 %**
Schwarz Holding GmbH	IABG-Mitarbeiterbeteiligungs AG

Total operating performance: about € 192 million* - Staff: approx. 1000

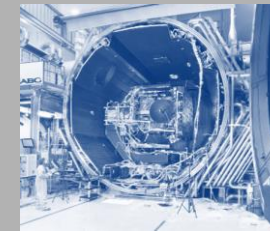| **Automotive**	**InfoCom**	**Mobility, Energy & Environment**	**Aeronautics**	**Space**	**Defence & Security**
Development and operation of mechatronic test systems for OEM & suppliers	Development and operation of secure ICT systems	Environmental solutions, protection, electro-mobility and change in energy policy	Fatigue strength tests for complete airframes and components	Operation of ESA coordinated Space Test Centres in Ottobrunn and Noordwijk	Operation of military simulation & test systems for analyses and conceptions

* Business year 2019

16 IABG Locations

IABG headquarters in Ottobrunn

Teleport

Automotive and airplane test center

Technology center

Environment

Space test center

Berlin

Oberpfaffenhofen

Koblenz

Dresden, Aeronautics

Lichtenau

Dresden, Geo Data Factory

Lathen

Noordwijk (NL)

AGENDA

Cybersecure satellite communications are a critical enabler of operations across Europe and global theaters

Sat Op1
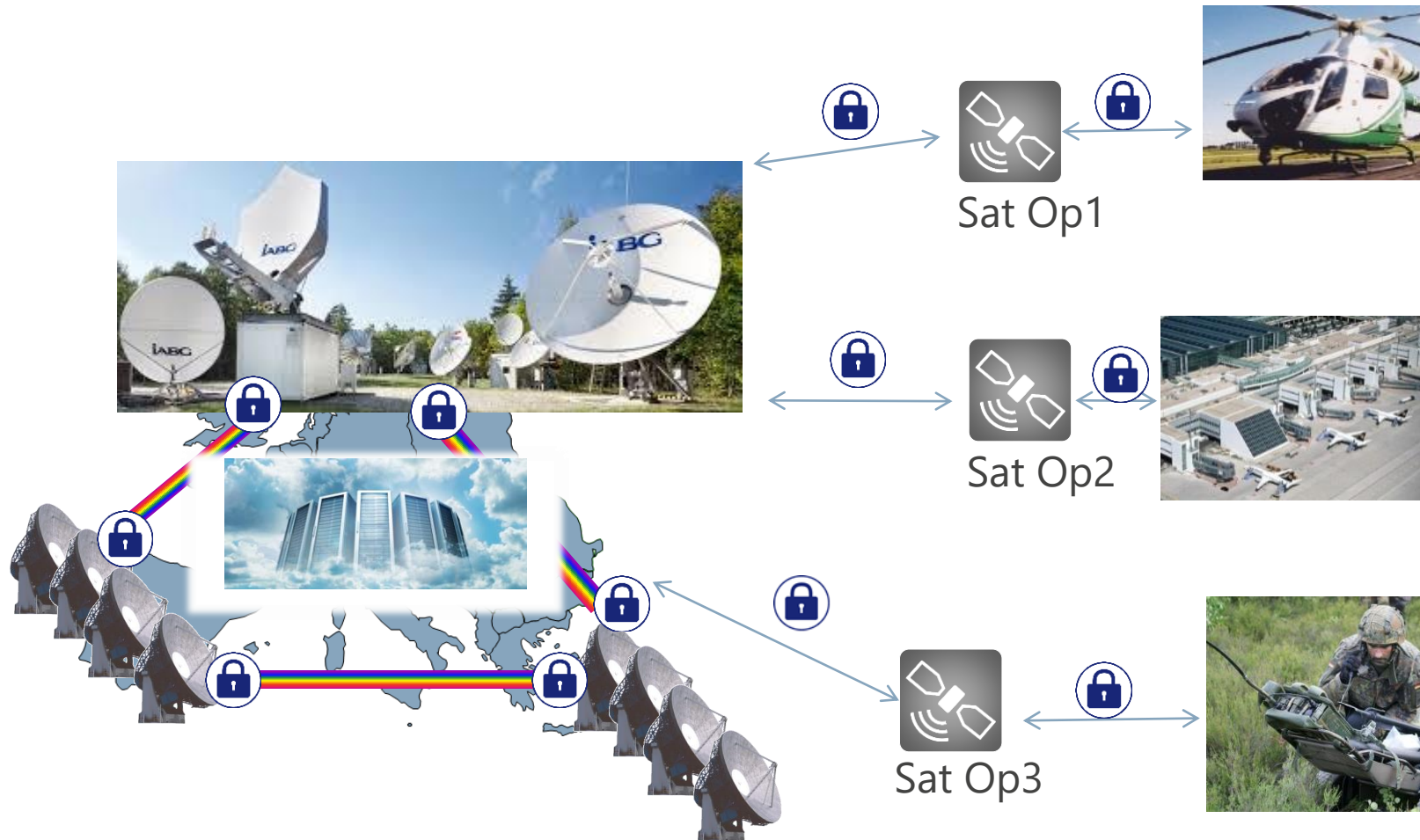
- Homeland Security
- Border Patrol
- Rescue
- ...

Sat Op2

- Critical Infrastructures
- Governmental Comms
- ...

Sat Op3

- (Non mission-critical) Military Comms
  - E.g.: MWR
  - NGO support

Picture credits: Die Welt, SAP SE

Common Criteria

Strategy: for use of Common Criteria (CC)-certified IT products/systems

- Level of overall Information Security depends also on the number of certified IT products and systems used in IT and satellite infrastructure.

- The identification of critical IT security components for space and terrestrial networks and assessment of these components (certification status) with regards to Common Criteria is a key factor.

- Drafting CC-Protection Profiles and CC-Security targets and closely following developments of new IT-components/systems w.r.t. to their impact on the CC evaluation status and later certification by the German BSI and other national authorities (crypto-approval) satisfies the users' security needs.

IT Components

IT Infrastructure
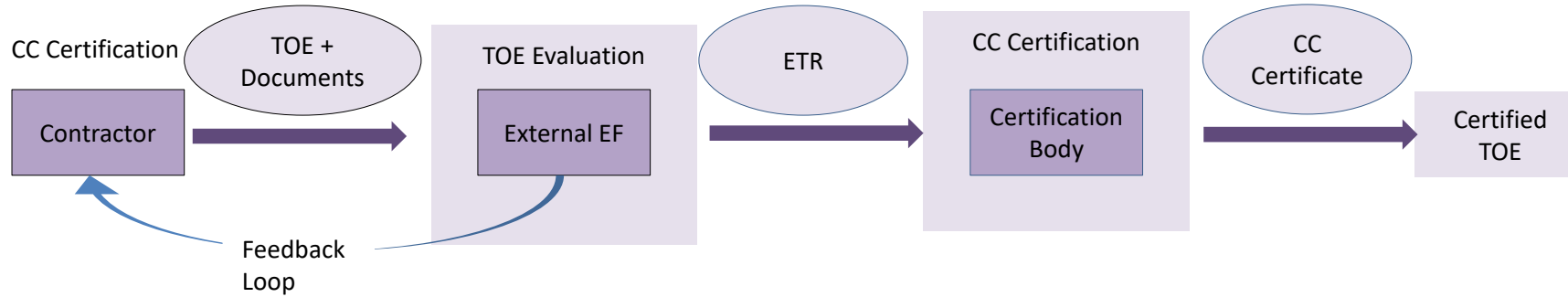
Certification iABG

Evaluation, certification and accreditation activities: Key objectives

- **Common Criteria (CC) Certification** for e.g.
  security sensitive components e.g. Security Modules HW/SW, etc.

    - Here: Certification Authority in Germany: BSI
    - Evaluation Facilities (>=EAL3): in Germany: HW-related: 3, SW: 6
- **Crypto Device Evaluation** / Approval (CDE)
  including coverage of Tempest certificates
    - Approval/Certification Authority: Germany: BSI
- **TEMPEST**
    - BSI, Other TEMPEST-approved facilities
- **AQUA** evaluation / approval process (EU level, between cert. authorites)

- Approval: EU/EC, National Certification Authorities
- Security Target (according to Common Criteria) as a key deliverable for Common Criteria
  evaluation and Crypto device evaluation
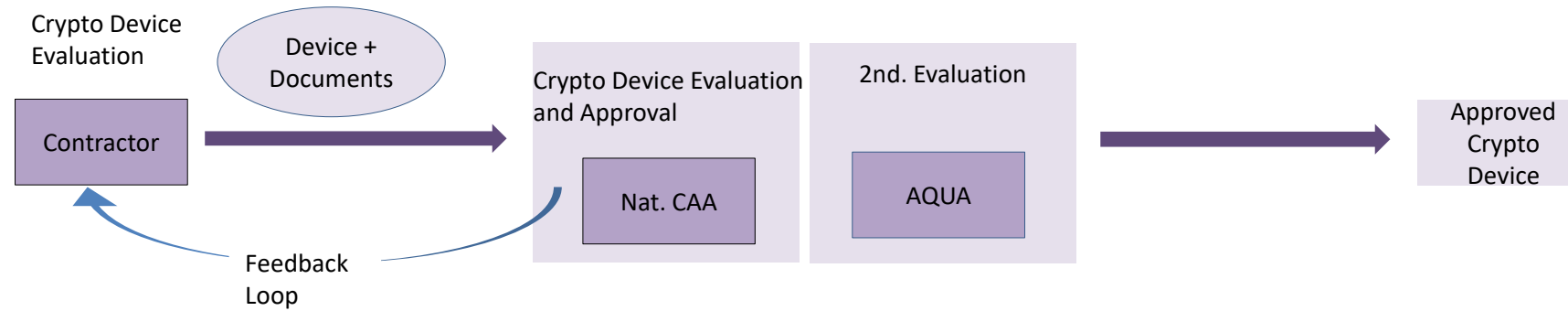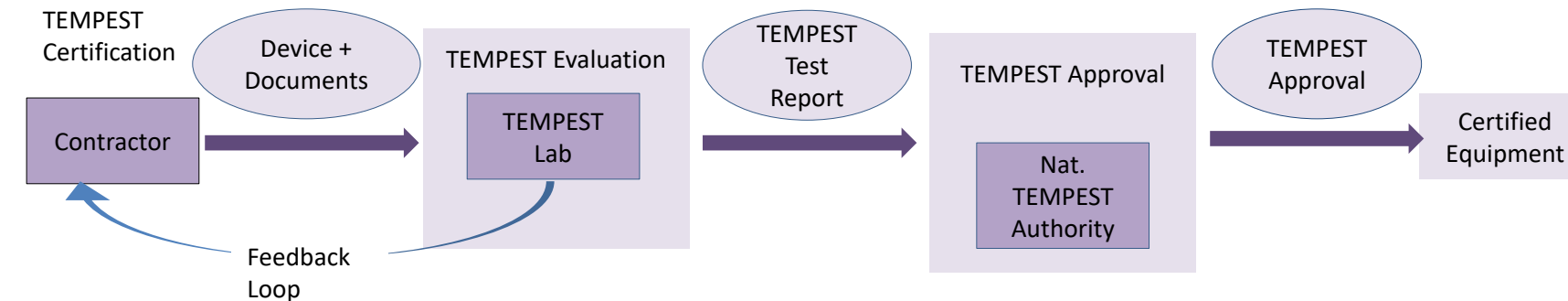- Use of Protection Profiles, where available and suitable

Certification Approaches for Common Criteria, Crypto, and Tempest

Schemes for types of evaluation, certification and accreditation activities (Germany and EU-level)

- **Common Criteria (CC)**
  - CC-Part 1-3 (ISO 15408), CEM
  - Germany-Scheme-specific: AIS of BSI Germany
  - CC-Specific: CCDB (Common Criteria Development Board) CC-specifics e.g. for Integrated Circuits, etc.
  - SO-GIS (Europe): Mutually recognition and recommendations for Cryptographic Devices, Security Boxes, ICs, etc.

- **Crypto Device Evaluation / Approval (CDE)**
  - BSI Guidelines for national classification levels

- **AQUA (Appropriately Qualified Authority): second evaluation / approval process (EU-level)**
  - "Shadowing"- Between Certification Authorities, EU TECH-P-01-02

These methodologies have been applied within SATCOM navigation and communications projects

IABG Accredited Test Center for ISMS, SatDSiG of BSI Germany

BSI accredited **Test Center** for
**ISO 27001/02 and
BSI IT Grundschutz:**

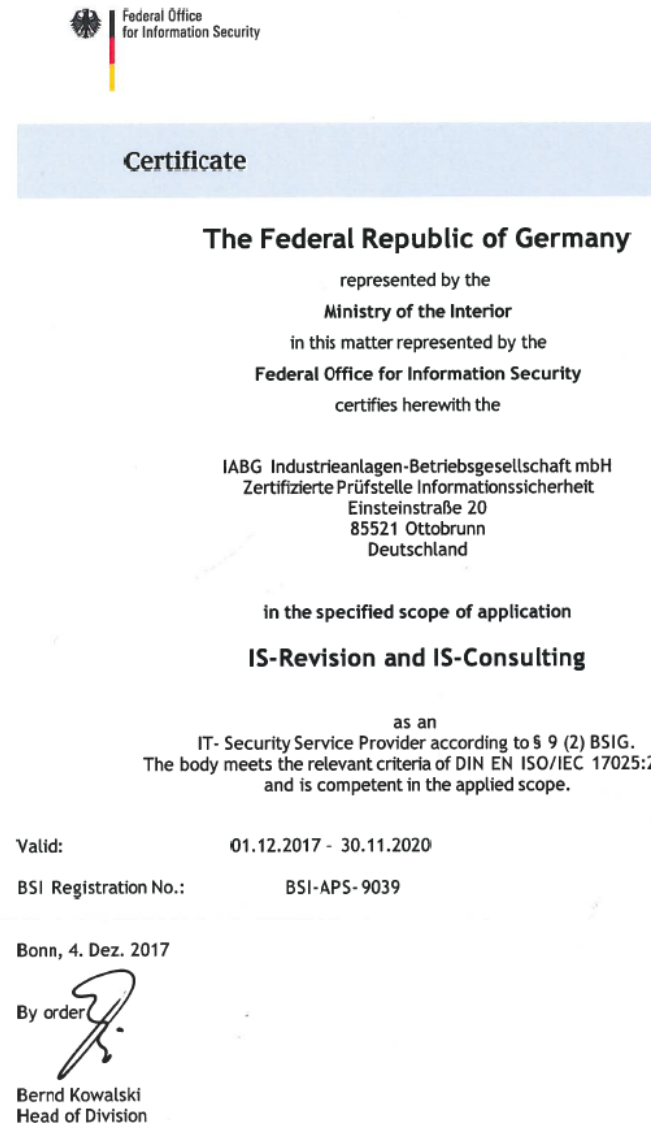BSI-Certified IT-Security Service Provider

IS-Revisor, IS-Consultants

ISO 27001-Auditors

Long term **Experience** with IT-Security, Safety and Management-Systems

Expertise of all relevant **Standards** und Regulations

Audits, IS-Revisions, Crypto Inspections & Security Expert Advice

iABG

IABG: BSI-accredited IT-Security Service Provider according to §9 (2) BSIG, Test Center,
        - Test Center for the Technical Guideline - Satellite Data Security Act (TRSatDSiG)

In addition to the security management and the creation of standard-compliant IT security concepts, the implementation of BSI IT Baseline Protection-compliant audits and the analysis, assessment of vulnerabilities targeted by cyber attacks are becoming increasingly important.

The Federal Office for Information Security (BSI) has officially certified IABG as an IT security service provider within the scope of Information Security (IS)-Auditing/ Revision and IS-Consulting.

- Audits and Consulting (Target: Auditor-Certificate „Entry level" or „Extended-" for the BSI-Certificate ISO 27001 on the basis of BSI IT-baseline protection)

- IS-revisions according to "Guidance for information security-revision" on the basis of IT-baseline protection of BSI and ISO 17025

- Operation and support of customer-specific audits and dedicated assessments (e.g. with accompanying Security Scans)

- Crypto inspections and security expert advice

- TRSatDSiG (Technical Guideline for **satellite** Data Security Act w.r.t. audits of ground segments, Guideline for security of high grade EOS-satellites operations)

Bundesamt für Sicherheit in der Informationstechnik

Certified IT-Security Service Provider

Certificate No:
BSI-APS-9039

Risk analysis and IT Security Concepts according to ISO 27001 on the Base of BSI 's IT-Baseline Protection and Enhanced Security
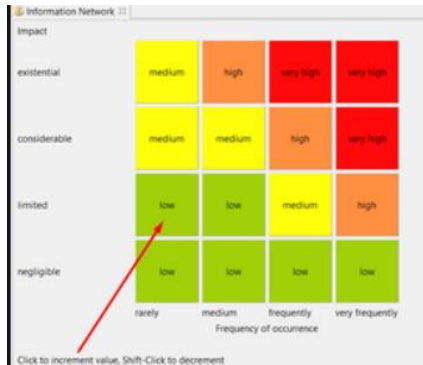
IABG associates security with compliance to law/regulations, continuity of operation of network infrastructures and the proactive protection against industrial espionage and theft of intellectual property.

We design, test and evaluate IT processes, systems, networks, according to European and worldwide standards and deliver customized security concepts.

We have the experience applying this expertise to GSA- & national satellite projects, e.g. Galileo PRS

Talk to the IABG consultants about current tasks:

- Risk analysis according to BSI-Standard 200-3, ISO 27005, ISO 31000, 31010 etc.

- Development of IT-security concepts according to BSI baseline protection (BSI-Standard 200-2, ISO 27001/2) and the military A 960-1
System specific security concepts (commercial, military)

- Production of IT-baseline protection –conformant modules for elevated/high security.

- Tool-based update of IT-security concepts

- Production and automation of reports

- IT-baseline protection trainings and Awareness-campaigns

- Selection, evaluation, experience w. tools (e.g. HiScout, EBIOS, crisam, Verinice)

- Security checks and criticality analysis (FMEA, Hazop etc.)

Your Points of Contact

Christian Creter

Senior Cybersecurity Lead

Constantin Schlachetzki

Program Manager Public Security

creter@iabg.de / schlachetzki@iabg.de

IABG
Einsteinstraße 20
DE-85521 Ottobrunn / Munich

Phone +49 89 6088-0
Fax +49 89 6088-2220, info@iabg.de , www.iabg.de

www.iabg.de/en/business-fields/infocom/satellite-navigation-satellite-communication/

www.iabg.de/en/business-fields/infocom/cyber-security/