Klausurtagung 2016
„Die SKB und ihre Partner in der Wirtschaft“

Funktionale IT-Sicherheitsarchitektur

für Einsätze der Bundeswehr

Workshop 2

Führungsunterstützungskommando

der Bundeswehr

STREITKRÄFTE BASIS

FITSA

Funktionale IT-Sicherheitsarchitektur für Einsätze der Bundeswehr

Ziel einer zukünftigen IT-Sicherheitsarchitektur

Ziel

- funktionale Forderungen an die IT-Sicherheit
- basierend auf Erfahrungen und Know-How
- technische Realisierungsmöglichkeiten

Win – Win:

Streitkräfte

- Integration innovativer Ideen im Bereich der IT-Sicherheit in die Beschreibung der Anforderungen
- Prüfung Machbarkeit bestehender Forderungen

Unternehmen

- transparente Sicht auf die durch die Streitkräfte erhobenen Anforderungen

STREITKRÄFTE BASIS

Motivation

„Wir kommunizieren so miteinander,

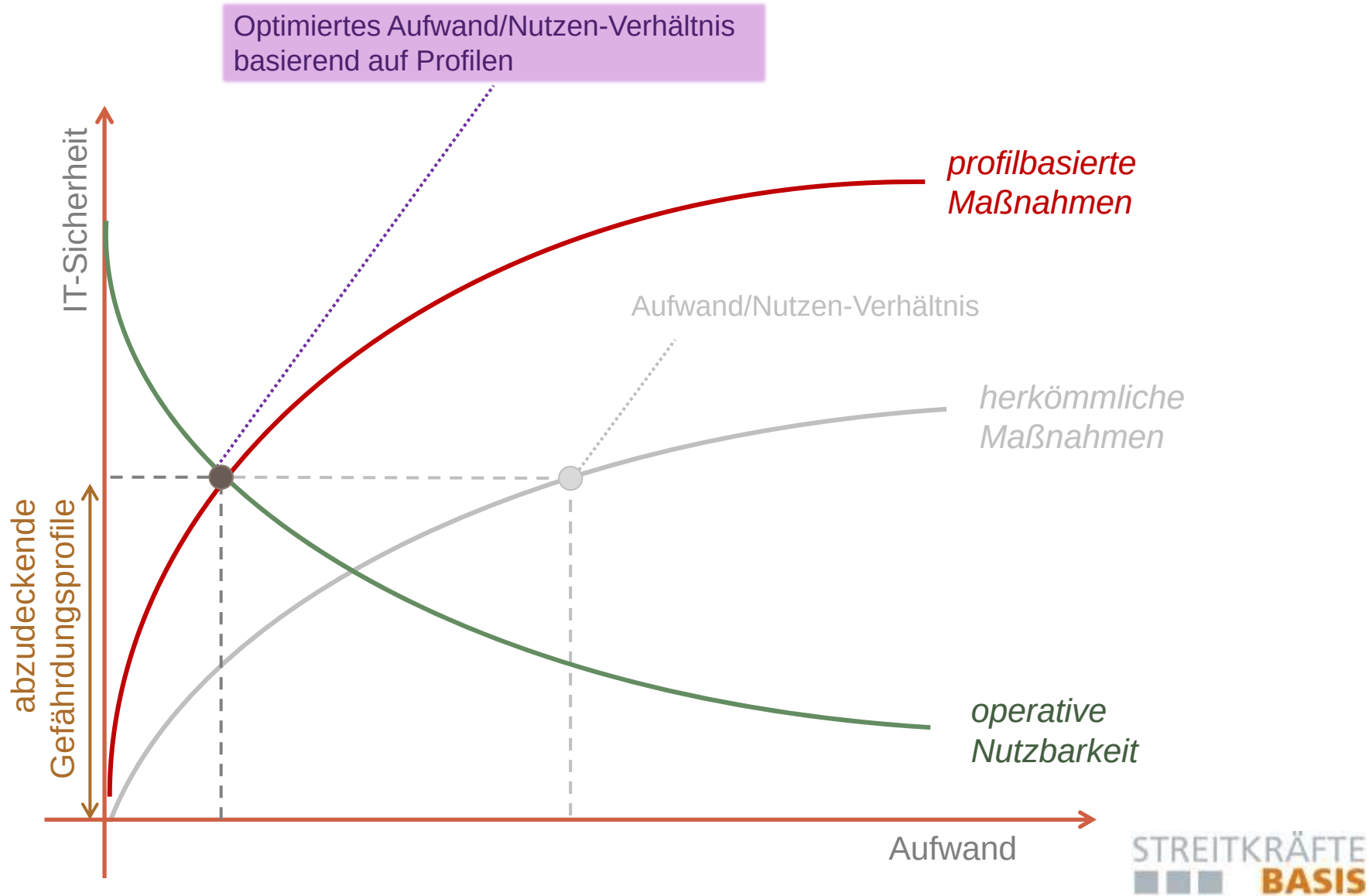
dass unsere Daten operativ nutzbar sind

und dennoch deren bestmöglicher Schutz

gewährleistet ist.“

STREITKRÄFTE BASIS

Profilbasierter Ansatz



Heutige Lage

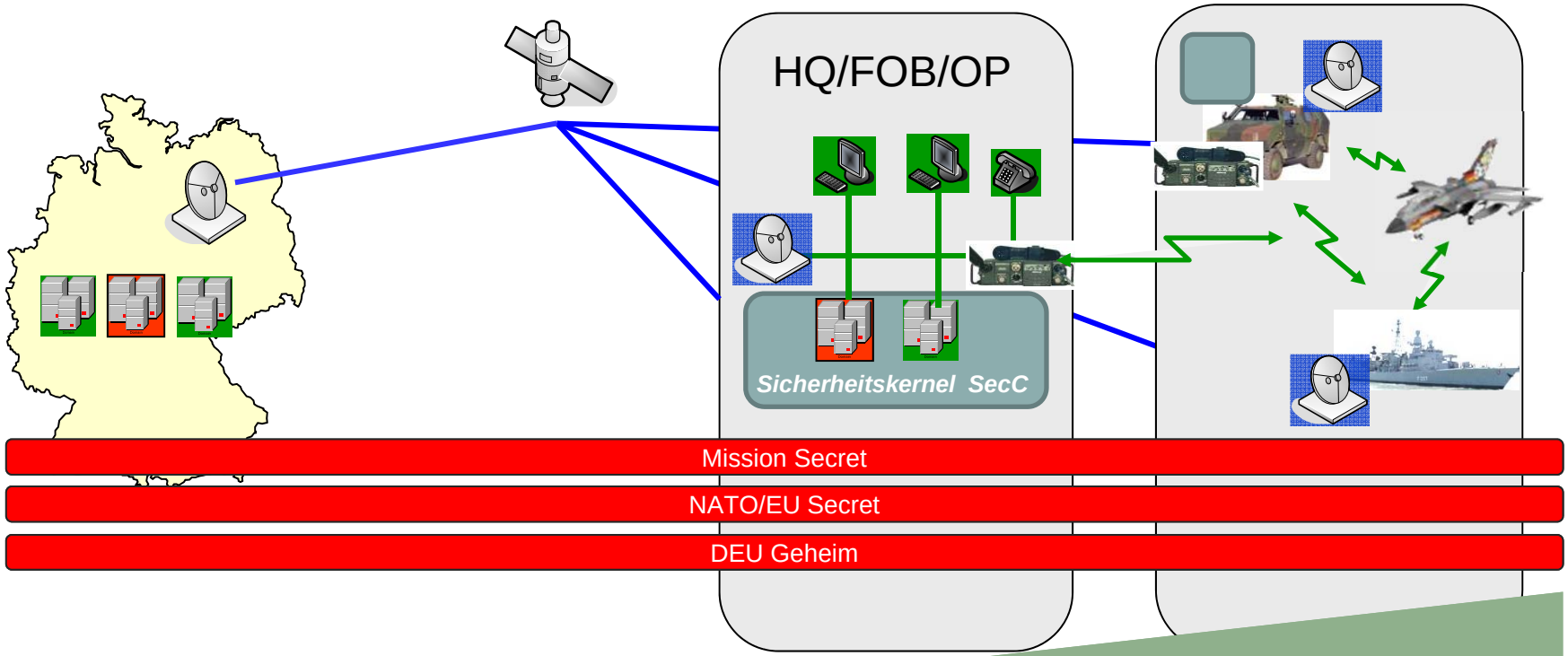
FüUstg für Dienststellen im In- und Ausland

Weitreichende Anbindung und Vernetzung

FüUstg für stationäre u. verlegefähige Einrichtungen

FüUstg für mobile Elemente

Bereitstellen von IT-Services



Ziel „FITSA“

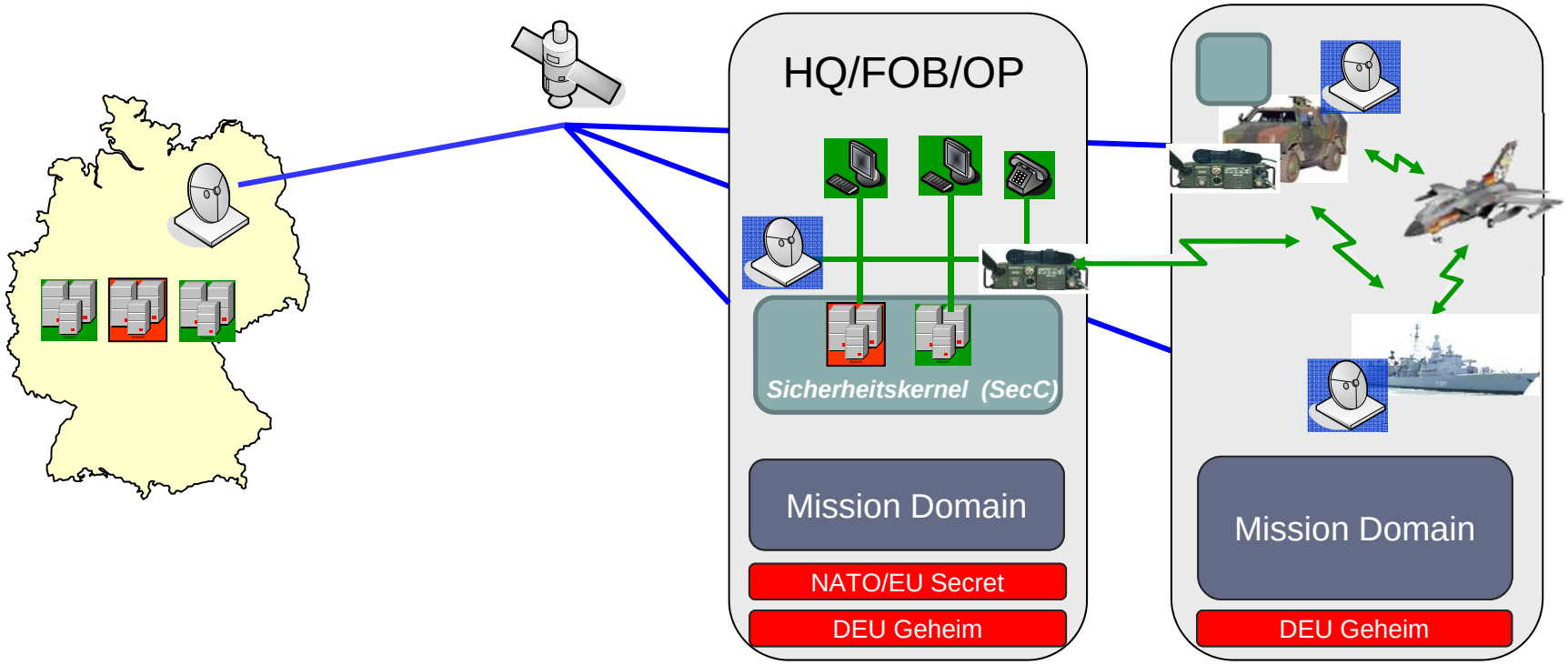
FüUstg für Dienststellen im In- und Ausland

Weitreichende Anbindung und Vernetzung

FüUstg für stationäre u. verlegefähige Einrichtungen

FüUstg für mobile Elemente

Bereitstellen von IT-Services



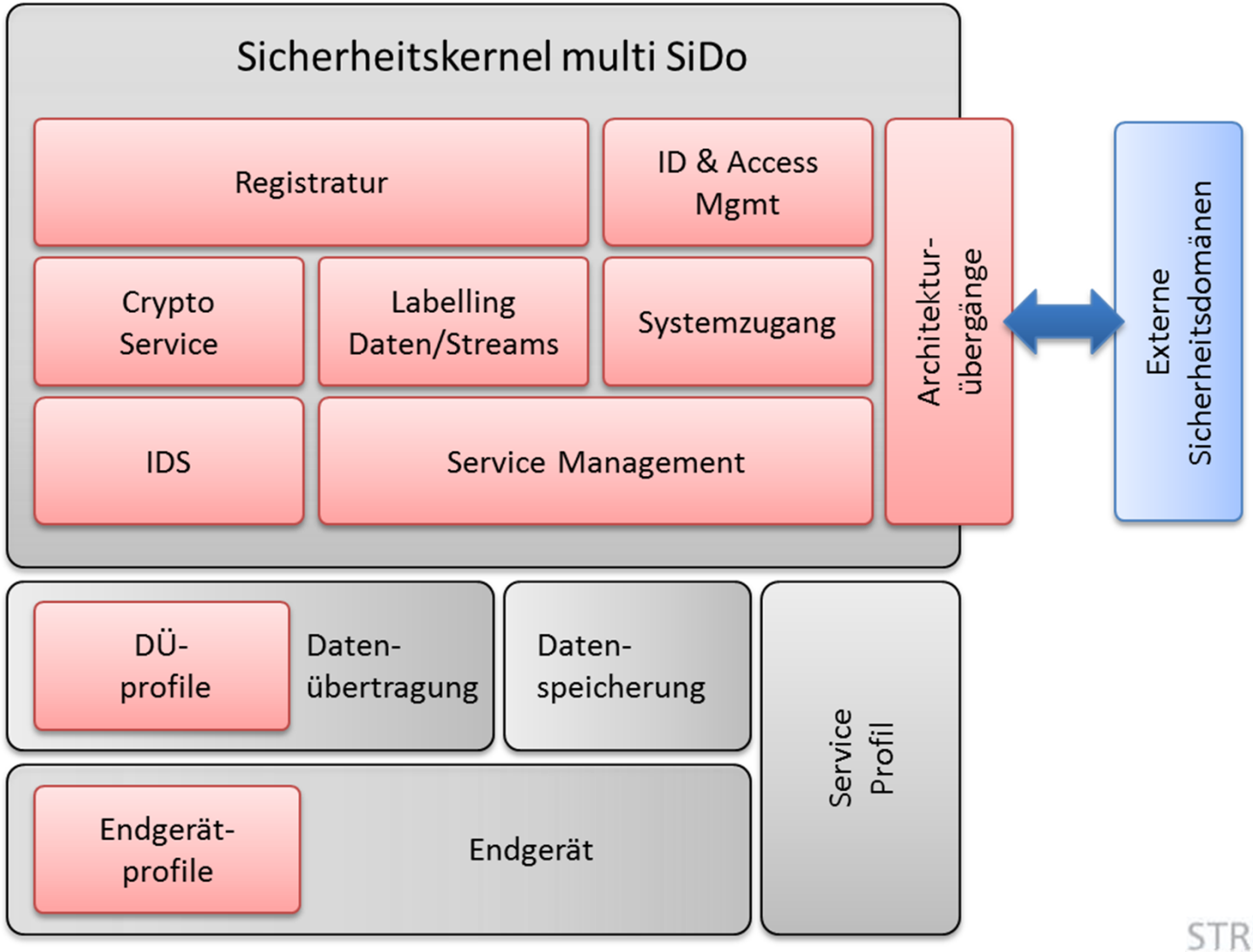
Gefährdungsprofil (GP) | GP | GP | GP | GP | GP | GP | GP | GP

Informationsdichte

Operative Anforderungen

OFFEN

Funktionale IT-Sicherheitsarchitektur



Aufbau des Dokumentes

Ziel des Dokumentes/ Einleitung/ Rahmenparameter

- Endgeräteprofile
- Anforderungen an die Datenübertragung
- Registratur
- Access & Identity Management
- Crypto Service
- Labelling
- Intrusion Detection System
- Service Management
- Systemzugang
- Domänenübergänge
- Anforderungen an externe Komponenten

Zusammenfassung

STREITKRÄFTE BASIS

Weiteres Vorgehen

- Zusammenarbeit zwischen Industrie und Bw fortsetzen und weiter ausbauen
- Einbeziehung anderer DstSt (PlgABw, BAAINBw, BSI, …)
- Einbringen Ideen/ Spezifikationen in FMN Management Organisation
  - Mission Secret Spezifikationen
  - Ende–zu–Ende Prozesse mit
    - offenen Standards
    - COTS Produkten
    - software-basierter Verschlüsselung
- Künftige Weiterentwicklung in der NATO

STREITKRÄFTE BASIS

Weiteres Vorgehen – Termine

- 20.06. – 24.06.2016: CWIX 2016 (Bydgoszcz, POL)
  - Vorbereiten Use Cases (Zusammenarbeit mit CAN) (Labelling/ Binding/ Trust Models)
- 24.10.2016: TIDE SPRINT #28 (VA, USA)
  - Teilnahme und Einbringen in Data-Centric-Security Track
- CWIX 2017
  - „FITSA“ Demonstrator
  - Multinationales Testing mit ersten Building Blocks (Labelling/ Binding/ Trust Models)

STREITKRÄFTE BASIS