
AUTOMOTIVE


INFOKOM


MOBILITÄT, ENERGIE & UMWELT


LUFTFAHRT


RAUMFAHRT


VERTEIDIGUNG & SICHERHEIT

11th International Conference on Availability, Reliability and Security (ARES 2016) – Workshop SecATM

A Model-Based Approach for Aviation Cyber Security Risk Assessment

Tobias Kiesling, Josef Niederl,
Jürgen Ziegler
IABG mbH

Matias Krempel
Deutsche Flugsicherung GmbH

DFS Deutsche Flugsicherung

IABG

Acknowledgement

- The results as presented are developed within the Air Traffic Resilience Project (Jan 2015 – July 2017) supported by the Free State of Bavaria

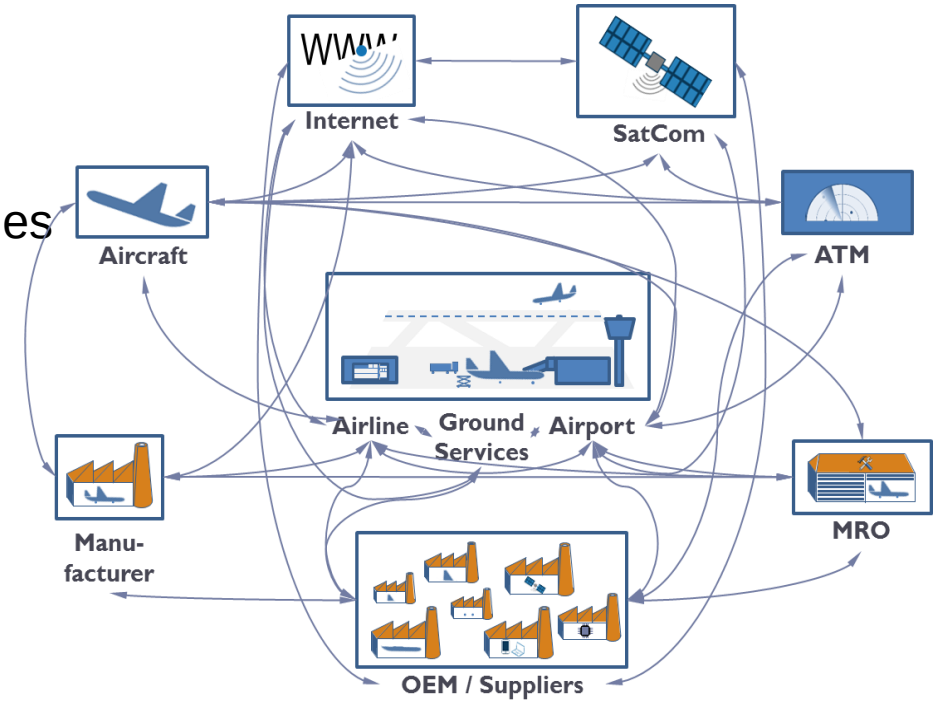
DFS Deutsche Flugsicherung IABG

Overview

- **Introduction and Motivation**
- Model Based Approach for Aviation Cyber Threat Risk Assessment
- Evaluation and Application
- Conclusions and Future Work

ATM Systems – Digitalization Trends and resulting challenges

- Increased automation and IT pervasion
  - ➢ Increasing attack surfaces and potentially decreasing robustness
- Harmonization of components
  - ➢ Increasing potential for re-use of attack tools and exploits
- Increasing system interdependencies
  - ➢ Propagation of risk between systems
  - ➢ Isolated security measures ineffective



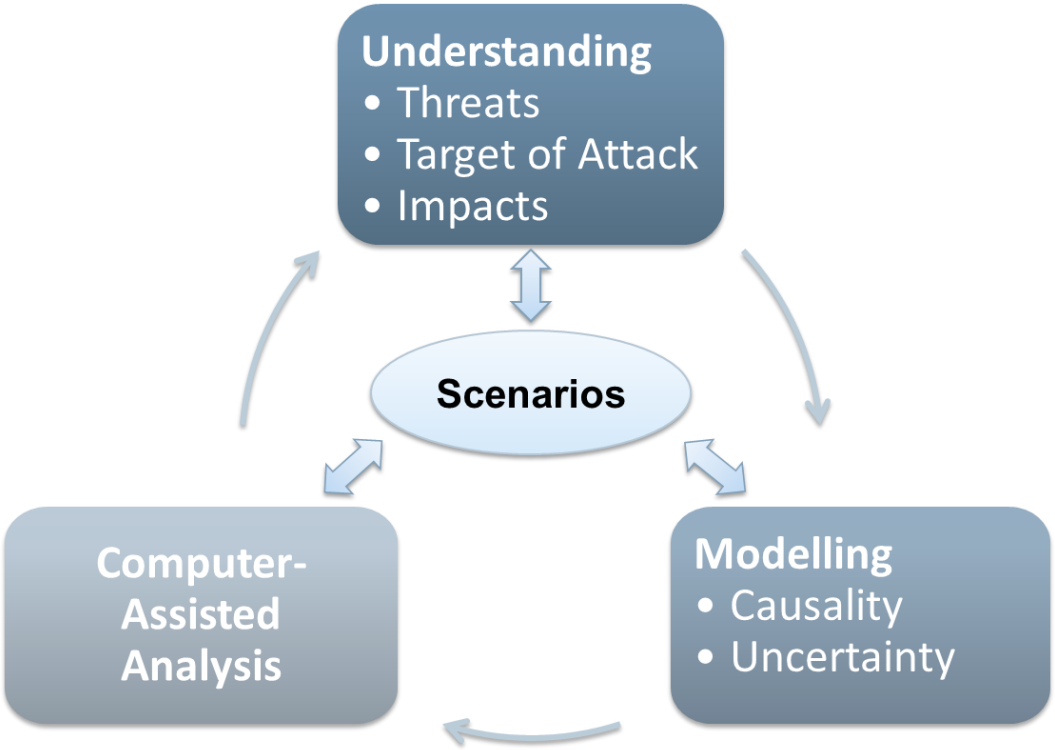
Source: Bauhaus Luftfahrt

Holistic and interdisciplinary understanding of threat and risk as basis for operational cyber resilience

DFS Deutsche Flugsicherung
IABG

Objective of the Approach

- Holistic Understanding of Threat and Risk Situation
- Model Based Approach
- Computer-Assisted Analysis / Reasoning
- Re-Use of Well Accepted Methods and Standards



Overview

- Introduction and Motivation
- **Model Based Approach for Aviation Cyber Threat Risk Assessment**
- Evaluation and Application
- Conclusions and Future Work

Model-Based Approach - Based on well-accepted foundation

Model of Attack

Based on STIX

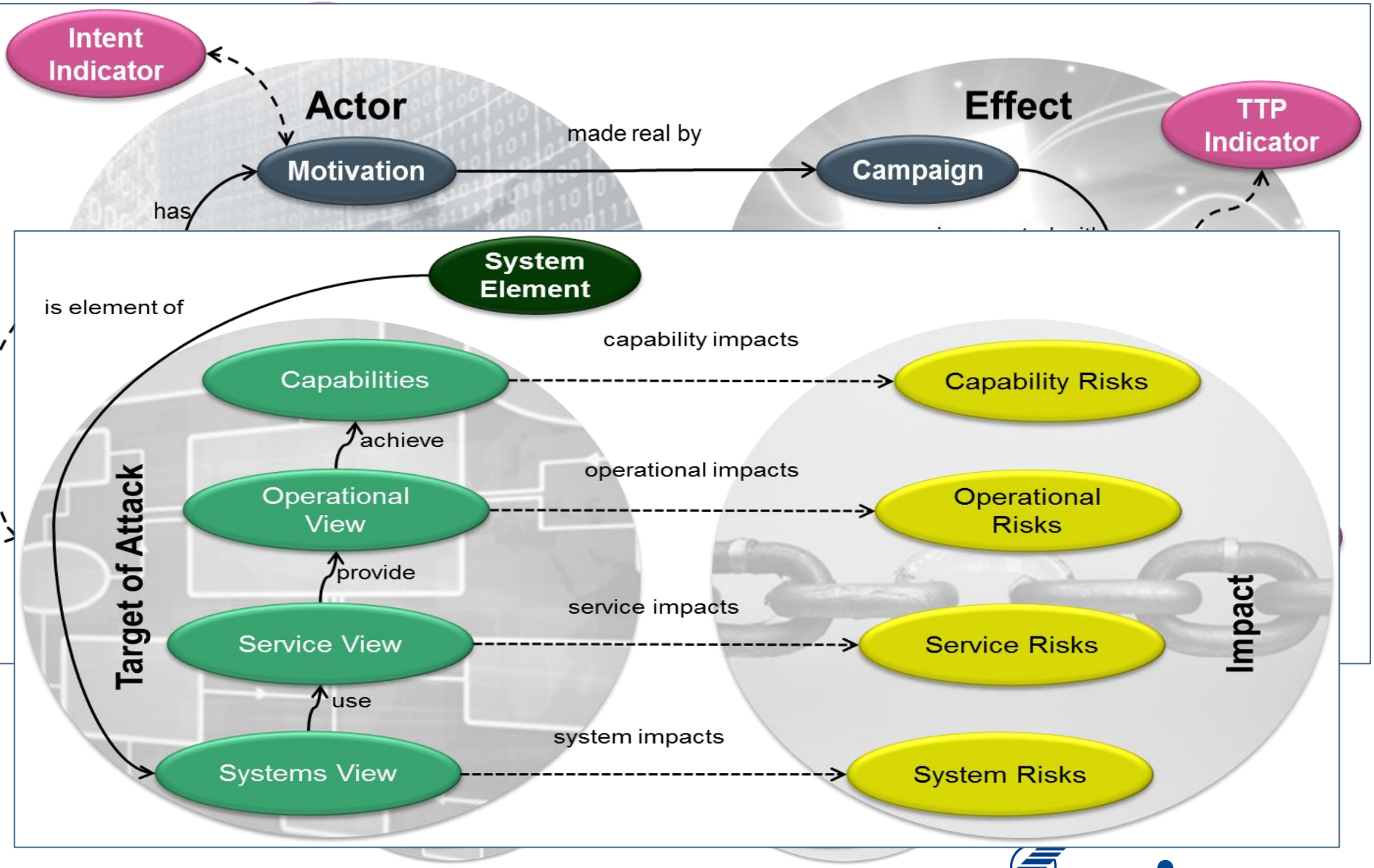
Model of Target of Attack

Based on EATMA

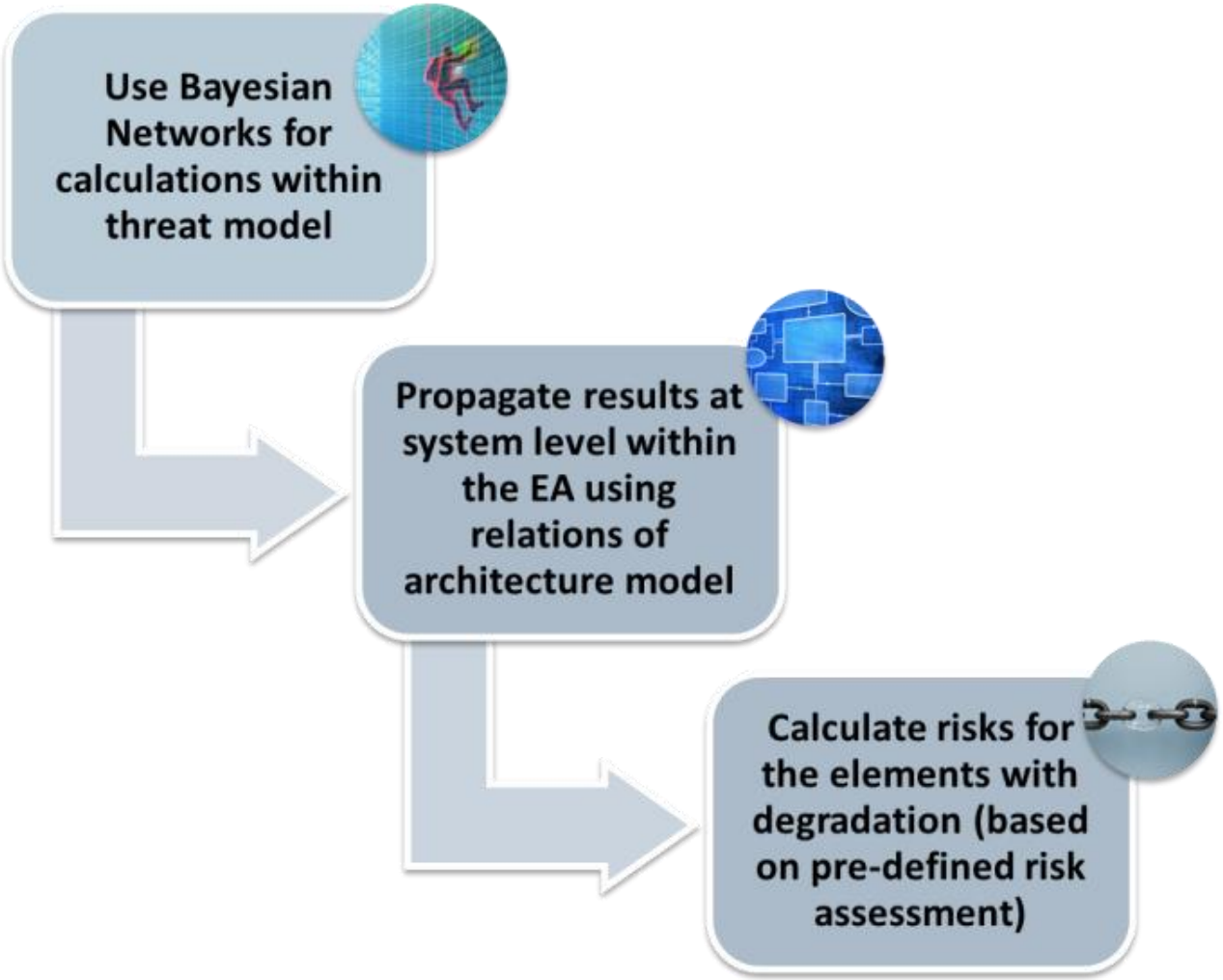
Risk Model

Connected to EATMA Elements

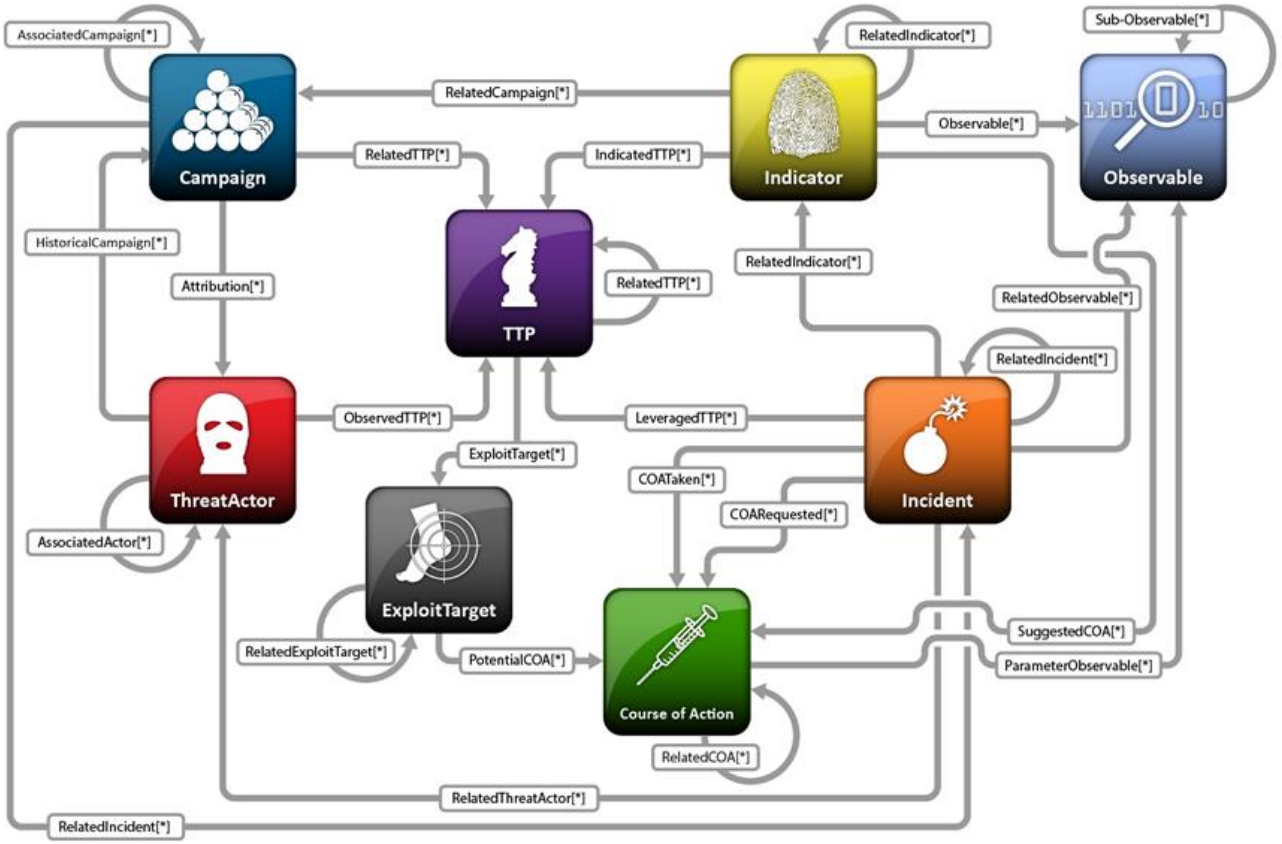
Generic Risk Model (simplified)



Computer Based Analysis / Reasoning

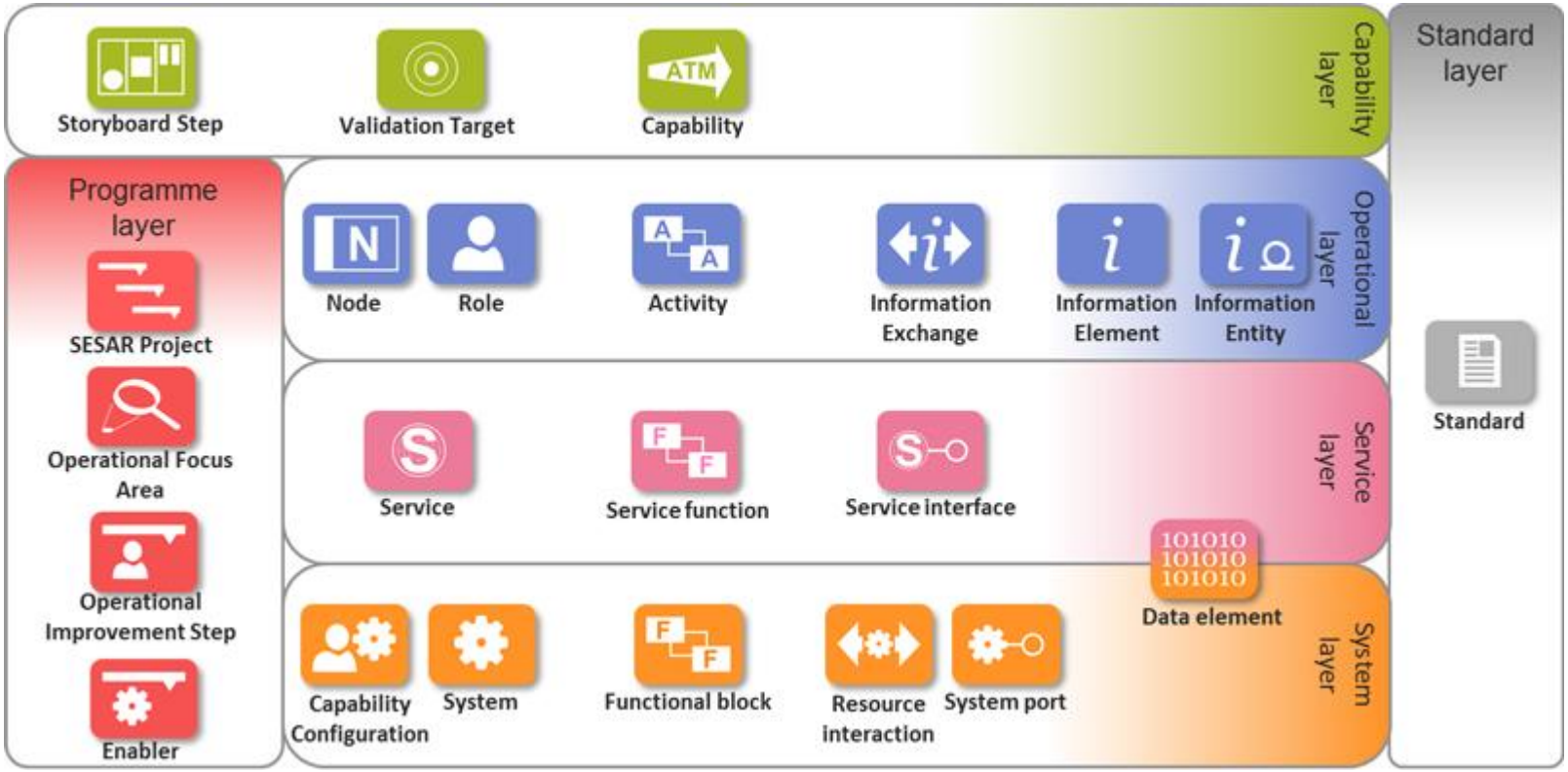


Re-Use of Well Accepted Standard - STIX



- Re-Use of Elements for Cyber Threat Description
- Basis for Information Exchange

Re-Use of Well-Accepted Method (Enterprise Architecture) => EATMA



- Re-Use of Subset of EATMA elements and relations
- Focus on System, Service, Operational and Capability Views
- Concretization of conceptual systems necessary

Concretization of Target of Attack => „KUNSTWELT“

Plan	Execute	Analyse

Demonstrator

The methodology as presented is implemented in a software demonstrator

Overview

- Introduction and Motivation
- Model Based Approach for Aviation Cyber Threat Risk Assessment
- ➢ **Evaluation and Application**
- Conclusions and Future Work

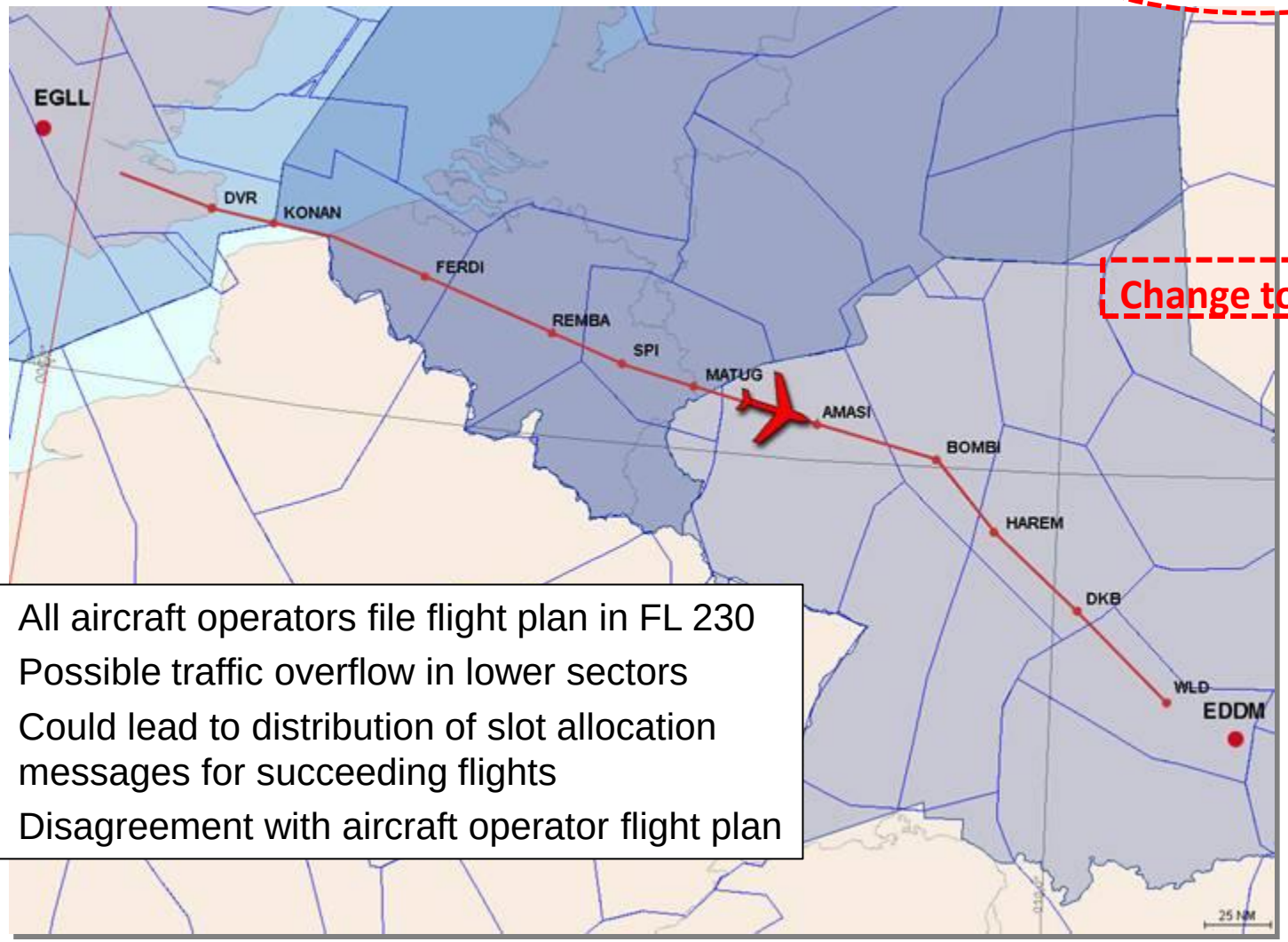
Evaluation and Application

Two evaluation and application scenarios:

1. Risk assessment and analysis for resilient process design
   - Scenario “Degradation of ATM Capacity”
   - Attack against strategic data flows
   - Exemplified with threat vectors against flight data flow

2. Dynamic situational picture - Detection and assessment of current threats
   - Attack against aircraft onboard systems
   - Implementation of exemplary threat indicator detection software
   - Data exchange using STIX formats

One Threat Example – Change of RAD restrictions



- All aircraft operators file flight plan in FL 230
- Possible traffic overflow in lower sectors
- Could lead to distribution of slot allocation messages for succeeding flights
- Disagreement with aircraft operator flight plan

RAD = Route Avaliabilty Document
FL = Flight Level

Overview

- Introduction and Motivation
- Model Based Approach for Aviation Cyber Threat Risk Assessment
- Evaluation and Application
- ➢ **Conclusions and Future Work**

Conclusions

Model-based approach

- Enable holistic understanding of cyber-threat related risk in aviation
- Apply computer assisted reasoning
- Integrate Know-how of interdisciplinary experts

Re-use of approved structures, elements and data

- Creation of big risk models with reasonable effort
- Sustainable due to the use of standard (STIX) and established model (EATMA)

Modern and solid approach for computer-based reasoning

Demonstrator is currently being implemented.

Recommendations for Future Work

Methods and Tools

- Enhance the maturity level of the demonstrator software
- Apply the methods to real life use cases and data
- Establish tools for continuous model maintenance
  - Automated read-in of attack models
  - Automated read-in of Enterprise Architecture models

Portfolio of models and data

- Develop portfolio of scenarios and models
- Integrate results of individual risk assessments
- Establish ATM-wide data exchange processes about threats including technical details based on STIX

Establish processes

- Processes for interdisciplinary cooperation to bring together the necessary domain expertise
- Integration in security management processes and structures

Questions?

Oversimplifications, progressively corrected in subsequent development are the most potent or indeed the only means toward conceptual mastery of nature.

Ludwig von Bertalanffy

Your Contacts

Tobias Kiesling, Josef Niederl, Jürgen Ziegler

IABG mbH

85521 Ottobrunn, Germany

e-mail: kiesling, niederl, zieglerj@iabg.de

Matias Krempel

Deutsche Flugsicherung DFS

63225 Langen, Germany

e-mail: matias.krempel@dfs.de

Backup…

The Case: Sharing of Flight Data

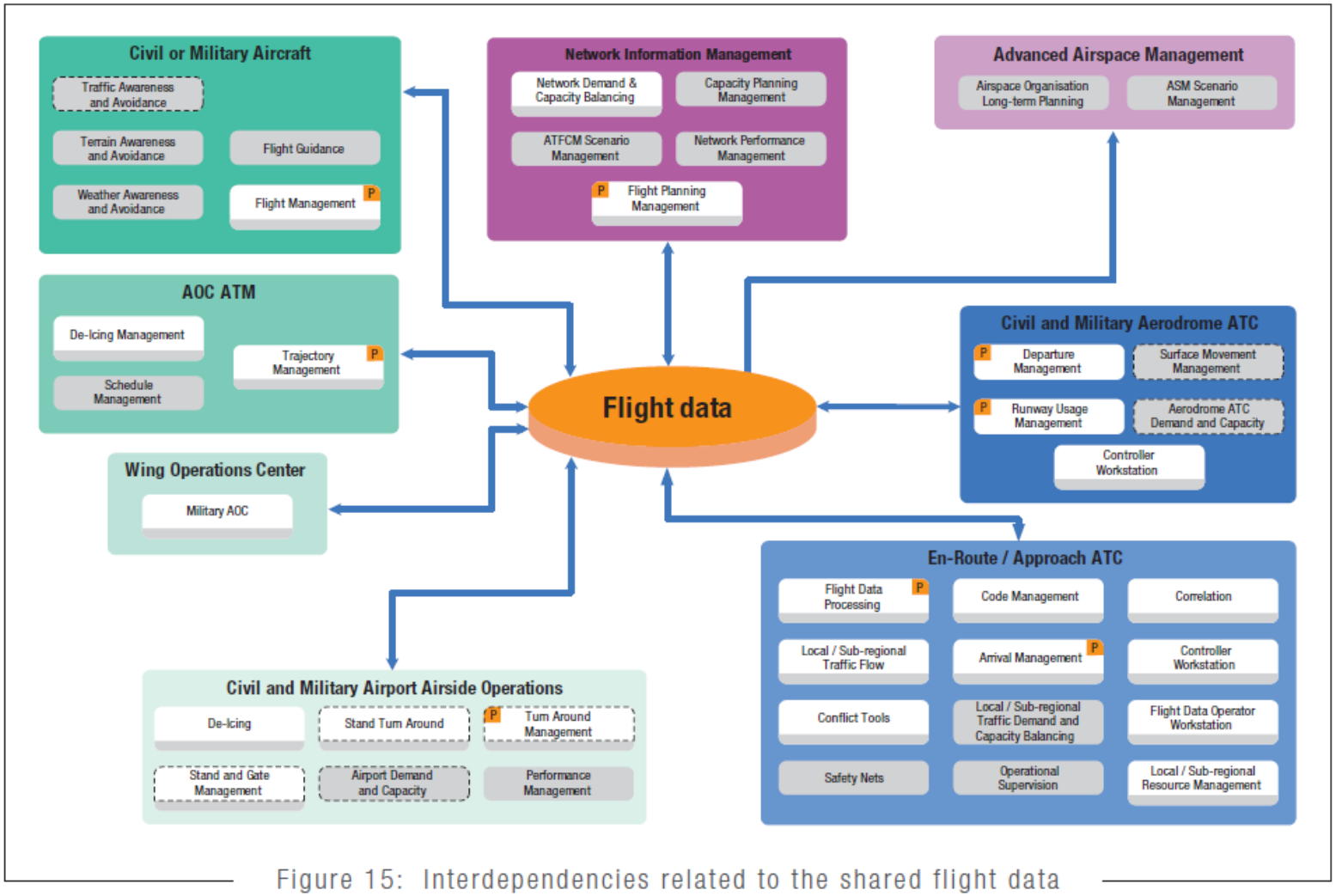
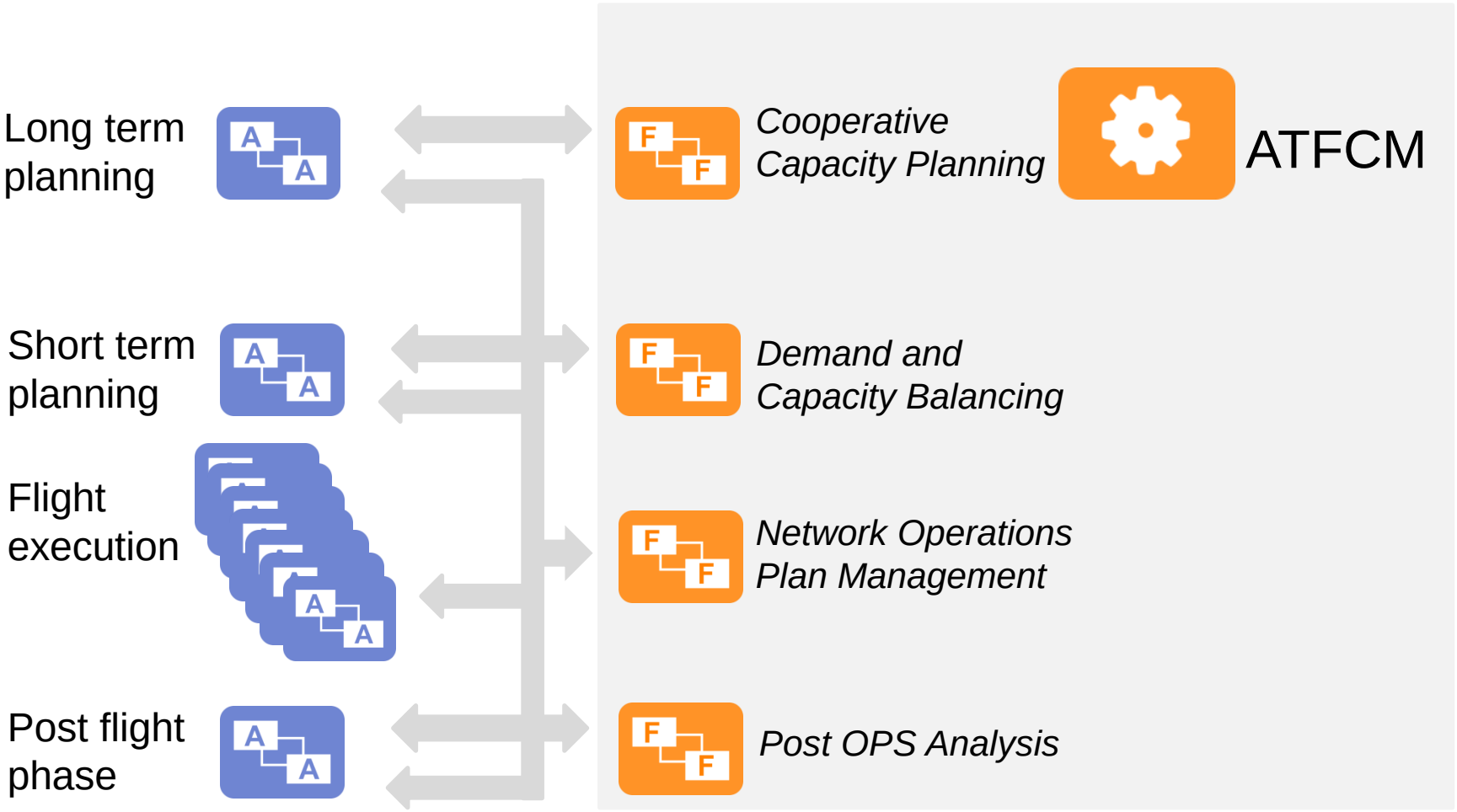


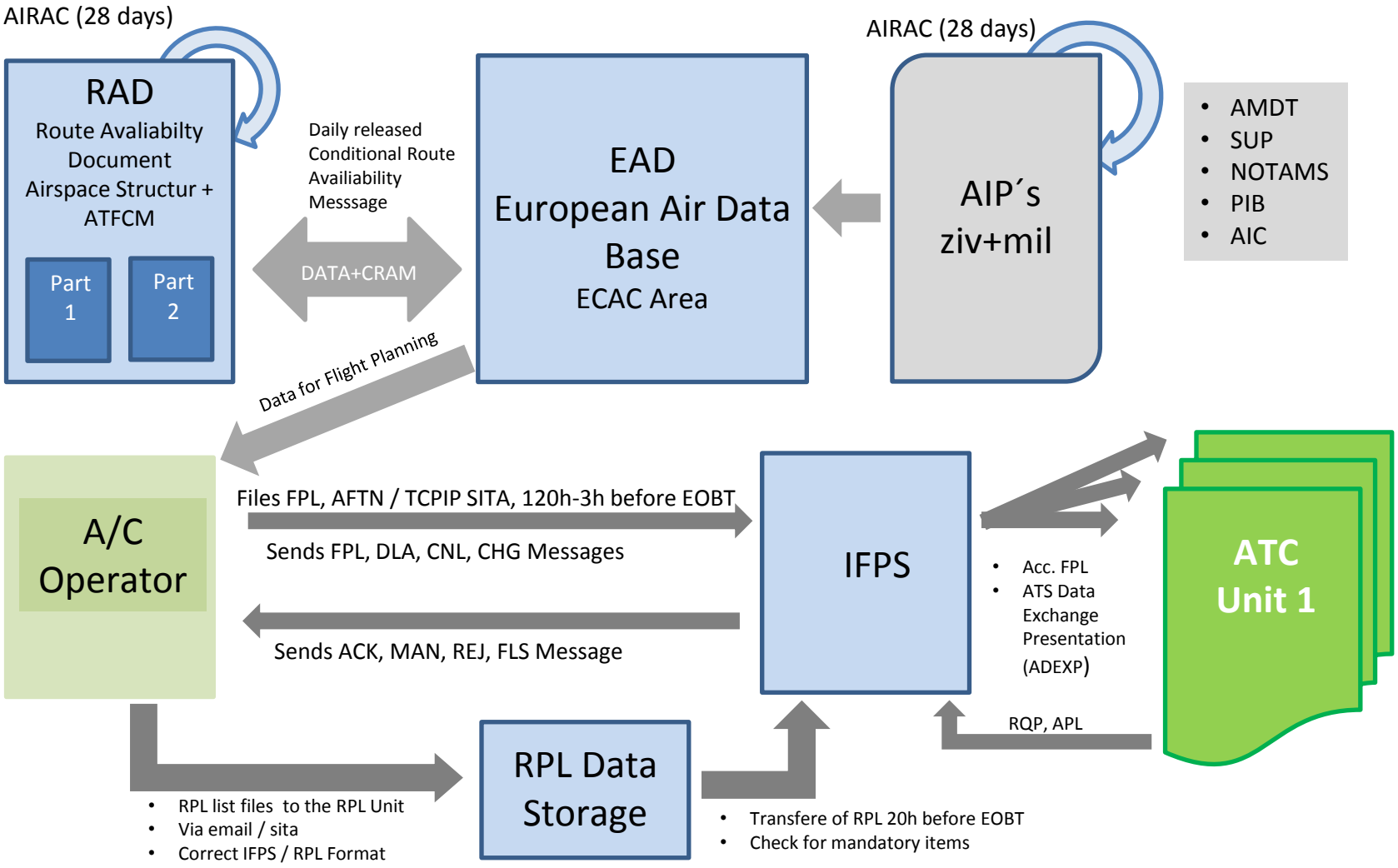
Figure 15: Interdependencies related to the shared flight data

Linking Architectures - Example



DFS Deutsche Flugsicherung
IABG

Flight Plan Data Process NM (CFMU)



Quelle: Cook, „EATM“