GERMAN AIRFORCE COMMAND

CODE 2020 I WORKSHOP 2
CYBER RESILIENCE OF CRITICAL INFRASTRUCTURES

CYBER-RESILIENCE IN COMPLEX OPERATIONAL SCENARIOS: AN ACTIONABLE SOLUTION APPROACH

11.11.2020, Munich

BUNDESWEHR

WHAT IS MAKING CYBERSPACE RELEVANT FOR FORCES?

What is the commanders critical information requirement according to cyberspace?

Cyber Resilience of Air and Space operations

The Air Force is operating in cyberspace, too…

… this requires cyber resilience

Objectives

- **Mission assurance in contested cyberspace**

Therefore:

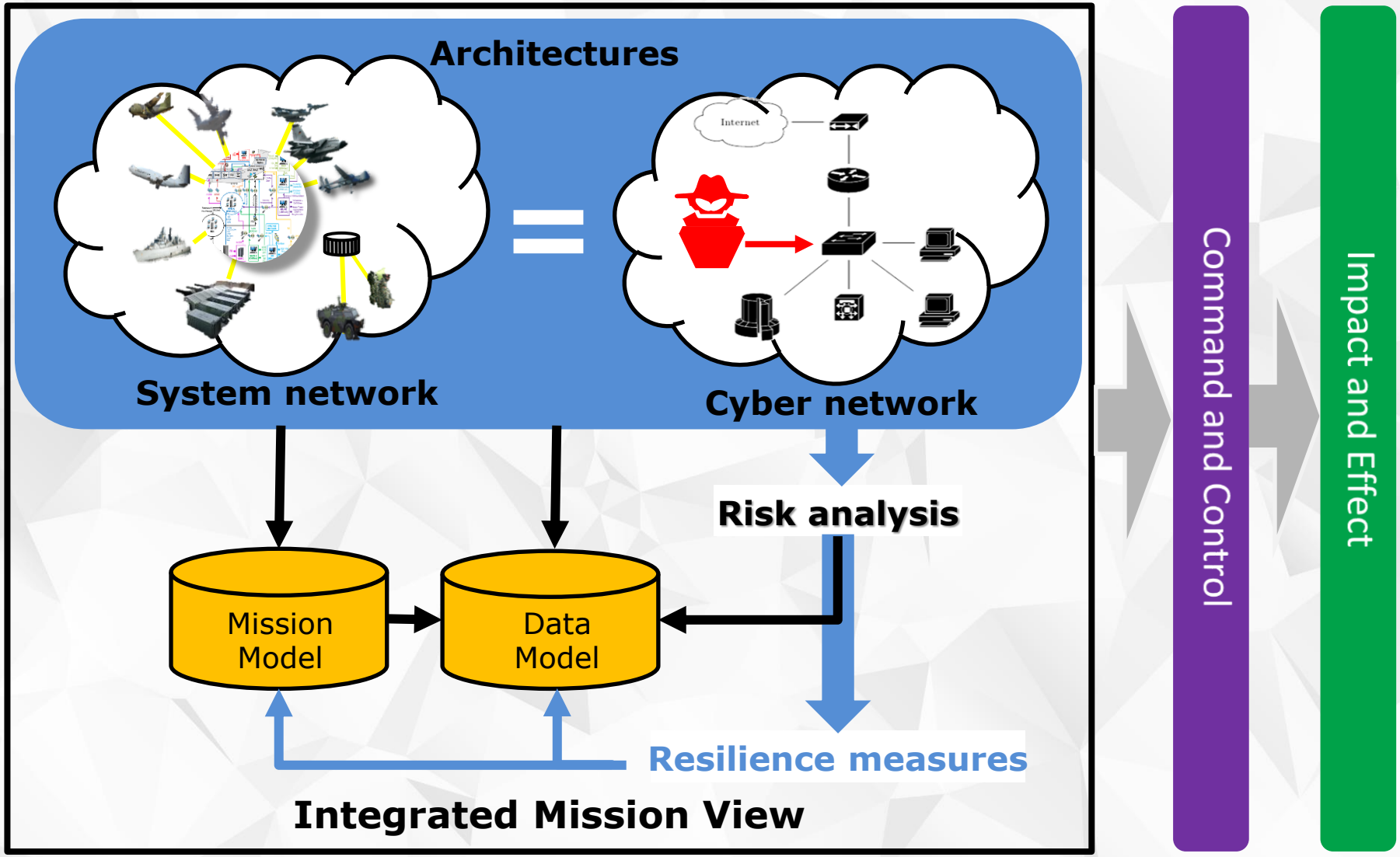
- Implementation of a dynamic assessment capability for cyber threats for all armed forces
- Increasing cyber resilience of Air Force weapon systems
- Increasing cyber resilience of the effect chains of air and space operations

Concept cyber resilience of air and space operations

- Assessment of vulnerability to (potential) cyber attacks
- Risk management for own network structures
- Measures for a robust and resilient IT infrastructure

→ **Setting preconditions for a capability-based dynamic cyber risk management for the German Air Force**

Cyber Resilience of Air and Space operations – the Concept

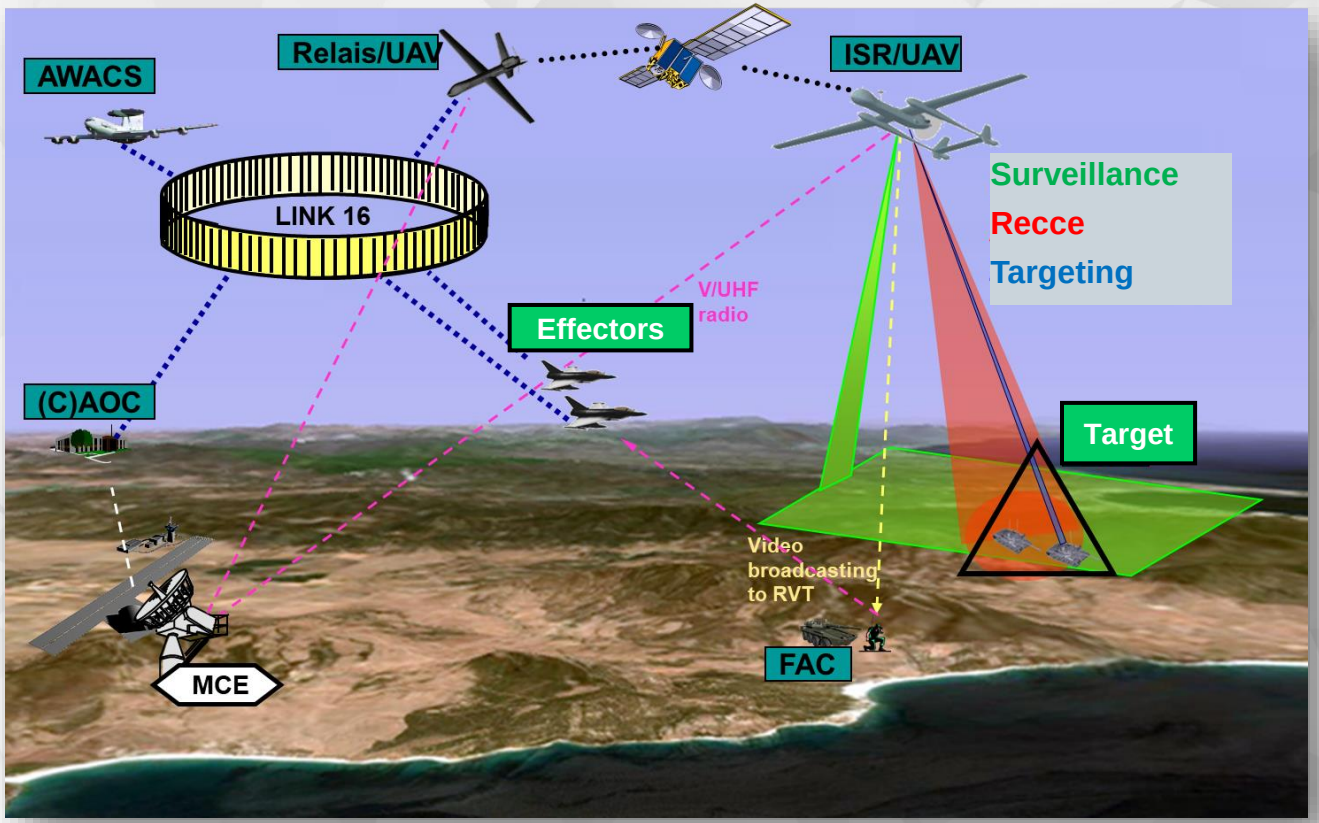


Mission module

Joint Fire Support

Effects chain (NOV-x)

- Who is involved?
- What are the information exchange requirements?
- What phases are there in theatre?

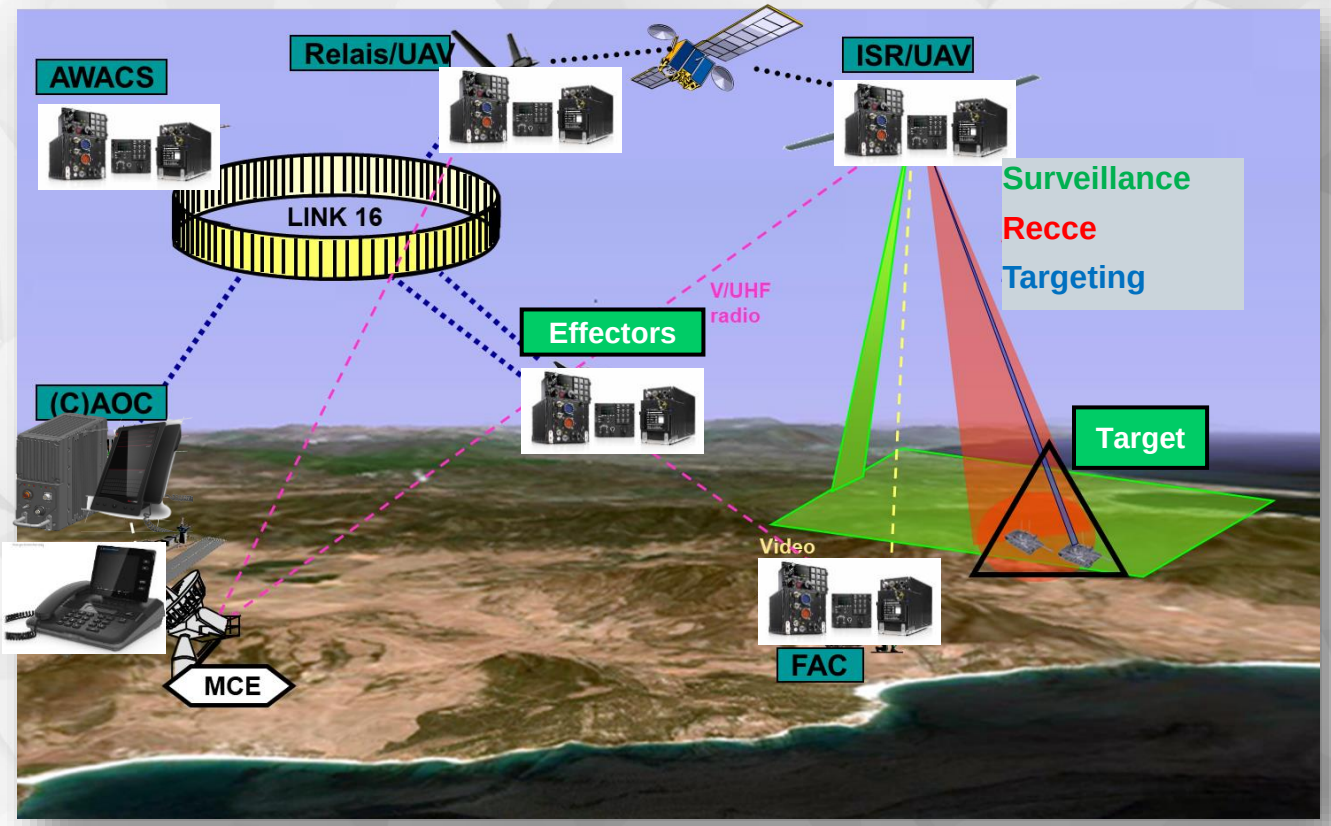


Cyber module

Architectures are creating benefits!

(NSV-y)

- Which communication systems are in use?
- Which interfaces are in use?
- Which protocols are in use?

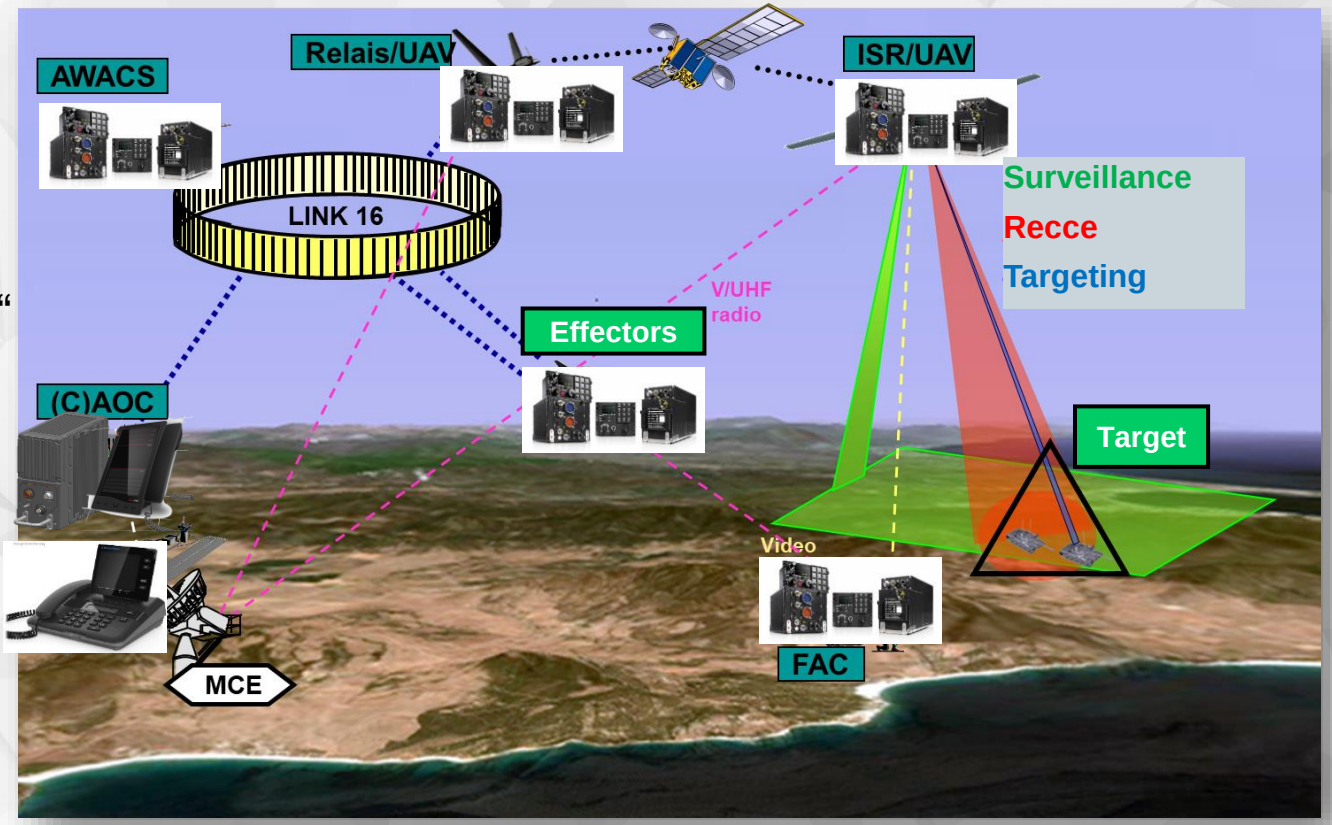


Vulnerability analysis & Risk assessment

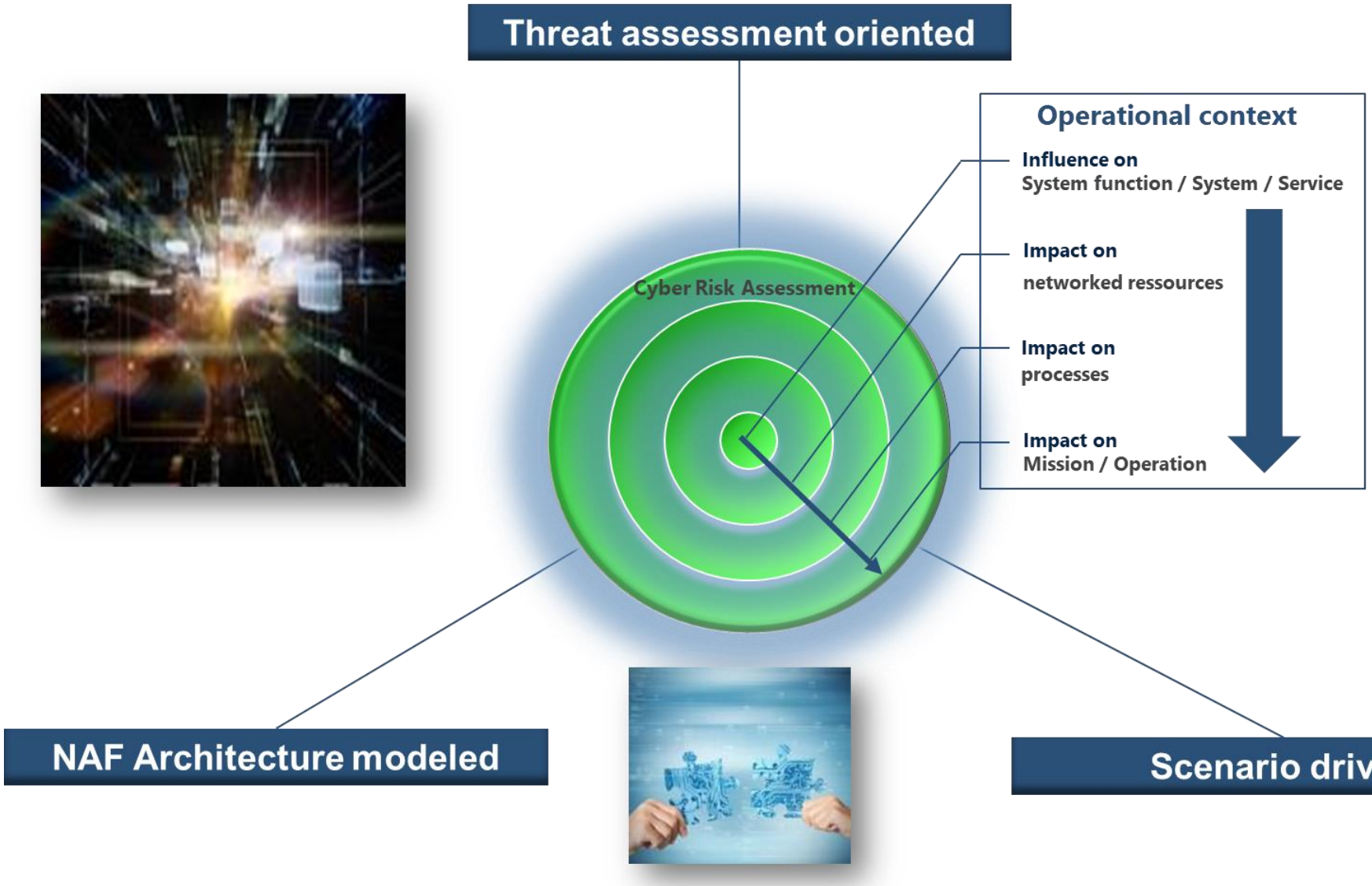
Benefit of architectures

- Vulnerability analysis for „mission critical chain links“
- Risk Analysis
- Resilience measures

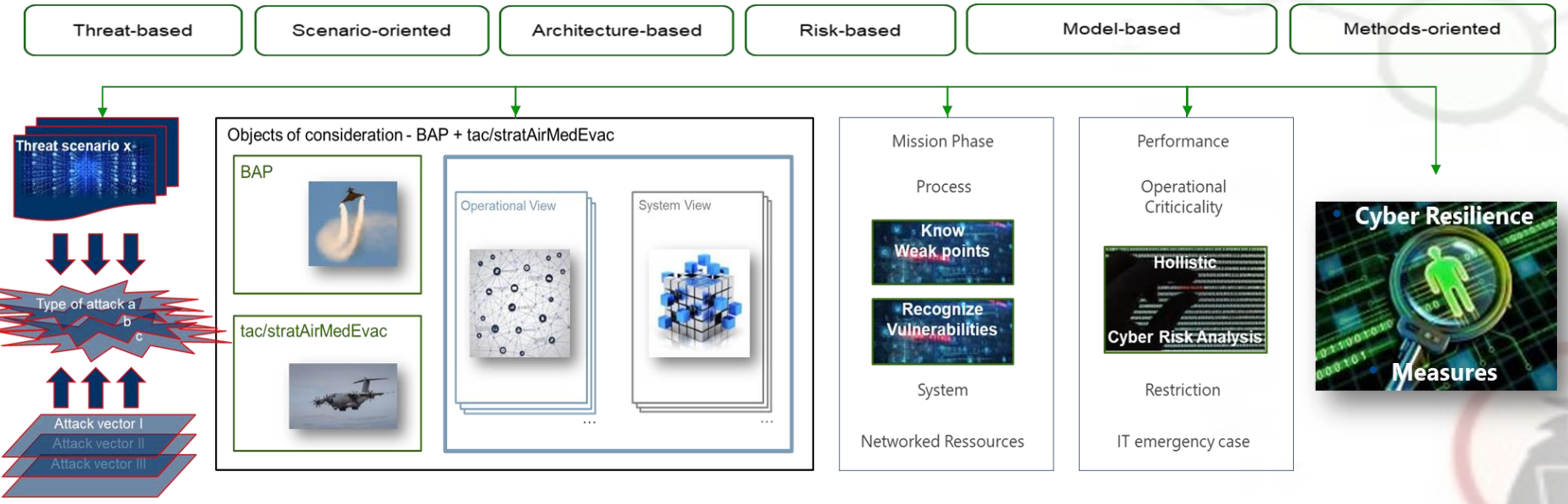
  (technical, tactical, procedural, organisational)



Taking the principle – Cyber-Resilience in complex Mission Scenarios



The holistic Cyber Resilience Process [operationalizable approach]



Develop Cyber Resilience process – operationalized & transferable concept

Interim results:

- NAF Architecture models ready to use.
- Architecture based threat assessment developed.
- Basic data (threat analysis) captured.
- Approach checked for plausibility.

In progress:

- Structure captured Basic Data.
- Construct attack model.
- Finalize Cyber resilence process model.
- Develop automating tools for architecture based threat assessment.

Conclusions:

- Solution statement positive, open to be operationalyzed, develop Tools for automating.
- Needs for further development: generating models and interaction between them also to be stored with automation.

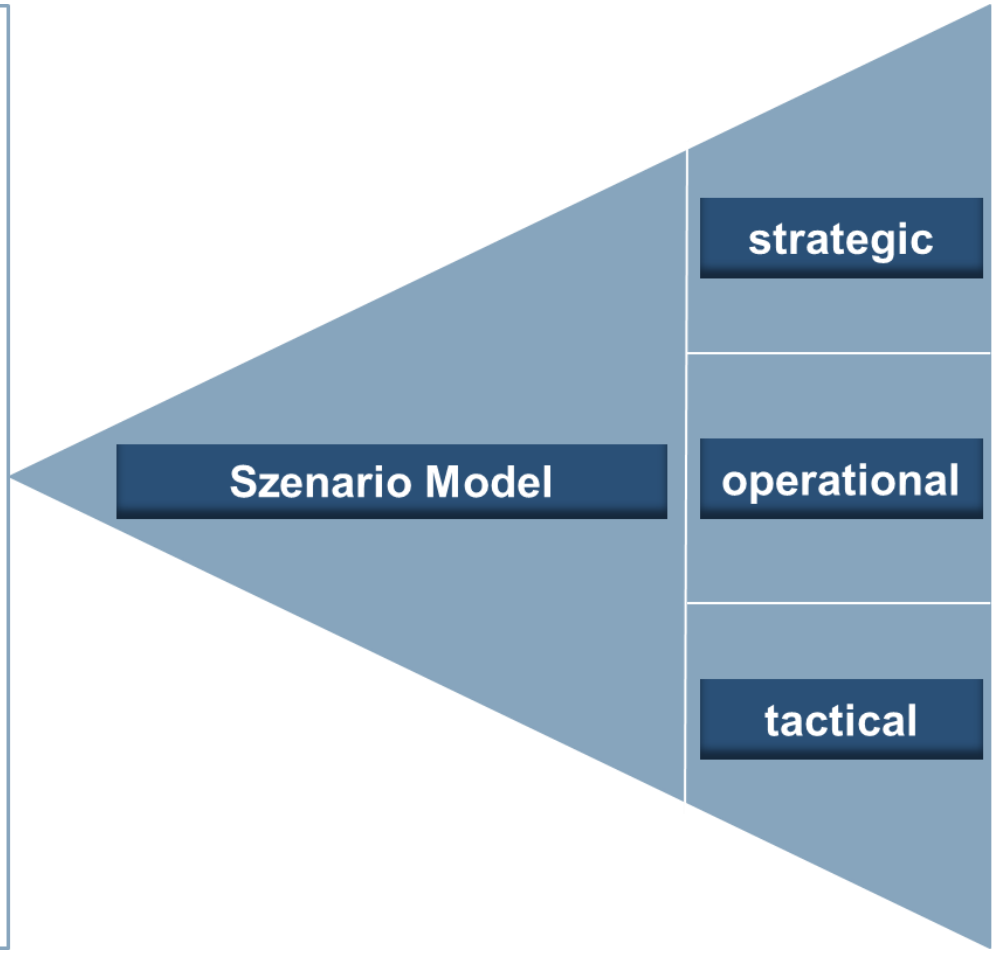
Outlook – a perspective view

Threat Model
- Logical threats
- Physical threats

NAF Architecture Model
- Organizational structure
- Operational structure
- IT-Infrastructure (functionally)

Network Architecture
- Technical
- Technological

Risk Model
- Cross-models
- Effect oriented
- Integrated and scaleable



Level of ambition:

Automating Models | dynamic Data Exchange in and between Models | Model based Analysis automated

Outlook – how to get progress: a perspective view

Threat Model
- Logical threats
- Physical threats

NAF Architecture Model
- Organizational structure
- Operational structure
- IT-Infrastructure (functionally)

Network Architecture
- Technical
- Technological

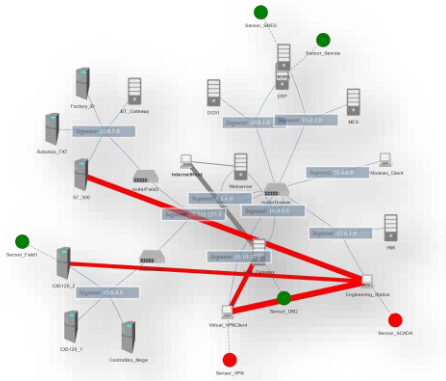
Risk Model
- Cross-models
- Effect oriented
- Integrated and scaleable

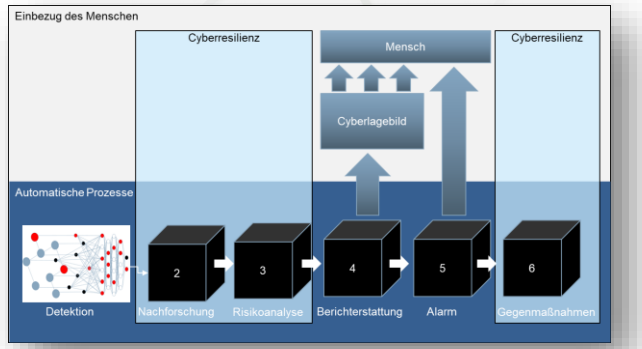
Szenario Model
- strategic
- operational
- tactical

Mature technology	&	Organization
Standards STIX and TAXII – attack model / data exchange		Basic principles – provide and foster Intelligence Preparation of the Cyber Space
„Standard" NAF / ADMBw – Models of threatened SoS		Reuse of Models
„Ergonomics" – capable operational picture		Provide Data exchange
Sensors – obeservation / indicators		
„Model Learning" – generate „AI-Models"		
Algorithm - Recognized Operational Picture & Assessment		

Added value of modules:

- Attack model / Data exchange
- Operational Cyber picture
- generate „AI modules"
- develope algorithm
- create operational picture
- process assessment





Conclusions – at a glance

Cyber-Resilience

Level of Ambition

Increasing the effectiveness of forces under cyber threats.

Therefore:

- Establishing of a dynamic asssessment capability of cyber threats in a combined approach
- Enhancing of cyber resilience of DEU Airforce weapon systems
- Increasing the cyber resilience of Air and Space operations effects chains

Concept of Cyber resilience of Air and Space operations

- Vulnerabilty assessment against potential cyber threats
- Risk management for own networks and structures
- Measures for robust and resilient IT-infrastructures

→ **Setting-up a capability-based dynamic Cyber- and IT-Risk Management for DEU Airforce**

Planning & Execution of Air and Space Operations

Quelle: IABG mbH, Diehl

Defence threats & mitigate risks in / on Cyber Space

Quelle: IABG mbH

Cyber Resilience - effects in network centric operations

Quelle: IABG mbH

Cyber-resilience in complex operational scenarios: an actionable solution approach

Thank you!

DEU AIRFORCE COMMAND

LtCol Sebastian Thölert

Senior Analyst Cyber Awareness

kdolw2IIIagrdsfuefae@bundeswehr.org

IABG Co

Gernot Schwierz

Senior Programme Manager Cyber Concepts & Operations

Schwierz@iabg.de