DEFENCE AND SPACE

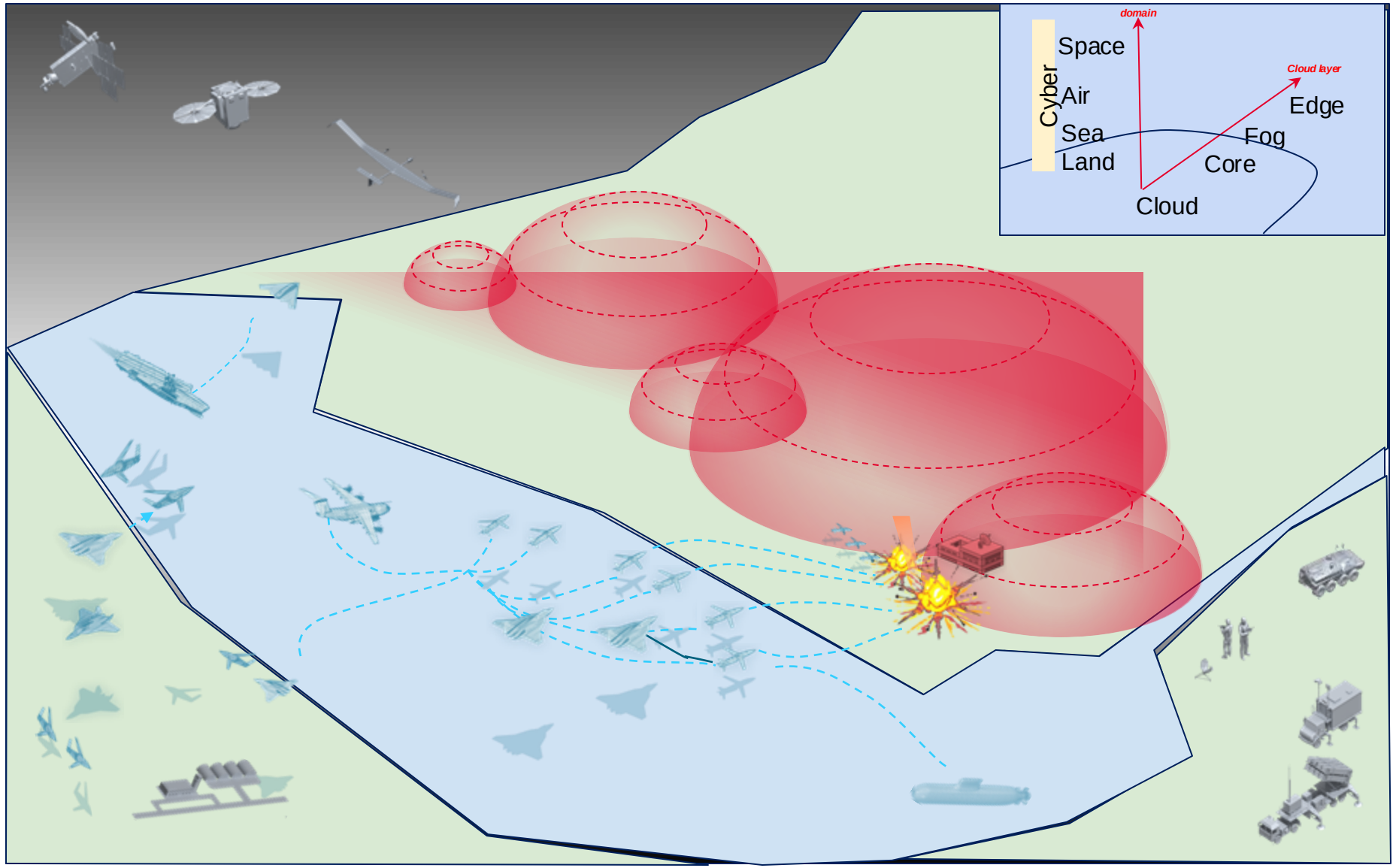
OC3 - Confidential computing study in the Multi-Domain Combat Cloud context

Edgeless Systems *"Any cloud always encrypted"*
Airbus Defence and Space *"Pioneering the future of air power"*

Lucia Jeschonneck, Luc Gallay

27 March 2025

AIRBUS



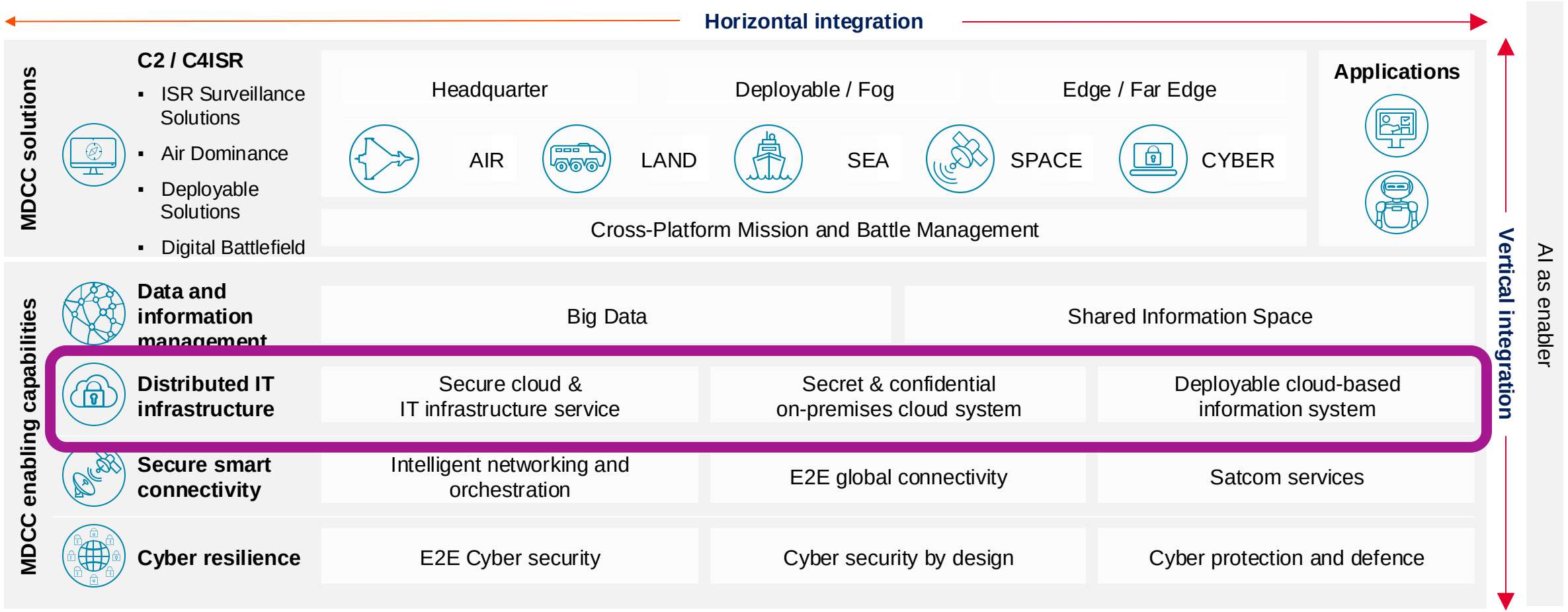
Multi-Domain Combat Cloud

Confidential computing to support:

- Sovereignty and immunity at core/cloud
- Cyber resilience at fog/edge

AIRBUS

Multi-Domain Combat Cloud system architecture abstract



AIRBUS

Software-defined defence and confidential computing: Joint study

Core / Cloud	Fog / Battlefield layer	Edge / X Platform
Communication and Information Systems Capabilities (IaaS / CaaS)		
Massive Intelligence Services	Common Operational Picture	Local / Group Operational Picture
Data Centre Services	Common Mission Data	Local / Group Mission Data
Core Services	Core Services	Core Services
Cloud Stack	Operating Systems, Cloud Stack	Operating Systems, Embedded OS
Data Centre HW	Ruggedized IT HW, Radios, Routers	Embedded HW, Ruggedized IT HW, Radios, Routers
Sovereign, immune, cyber resilient IT infrastructure		
Secure cloud and IT Infrastructure Services STACKIT IONOS OVHcloud DELOS CLOUD SAP	Confidential on-premises systems Deployable cloud-based information systems	
Edgeless Systems *"Any cloud always encrypted"*	**Confidential Containers with Contrast, AMD SEV / Intel TDX**	

Protecting mission data against significant threats with confidential computing

Physical loss: Data remains encrypted in memory, making access by enemies difficult.

Compromised infrastructure: Remote attestation ensures workload integrity, even when vehicle, command & control or network are compromised.

Insider threats: Unauthorized access or manipulation by administrators is mitigated with remote attestation and policy enforcement through Contrast.

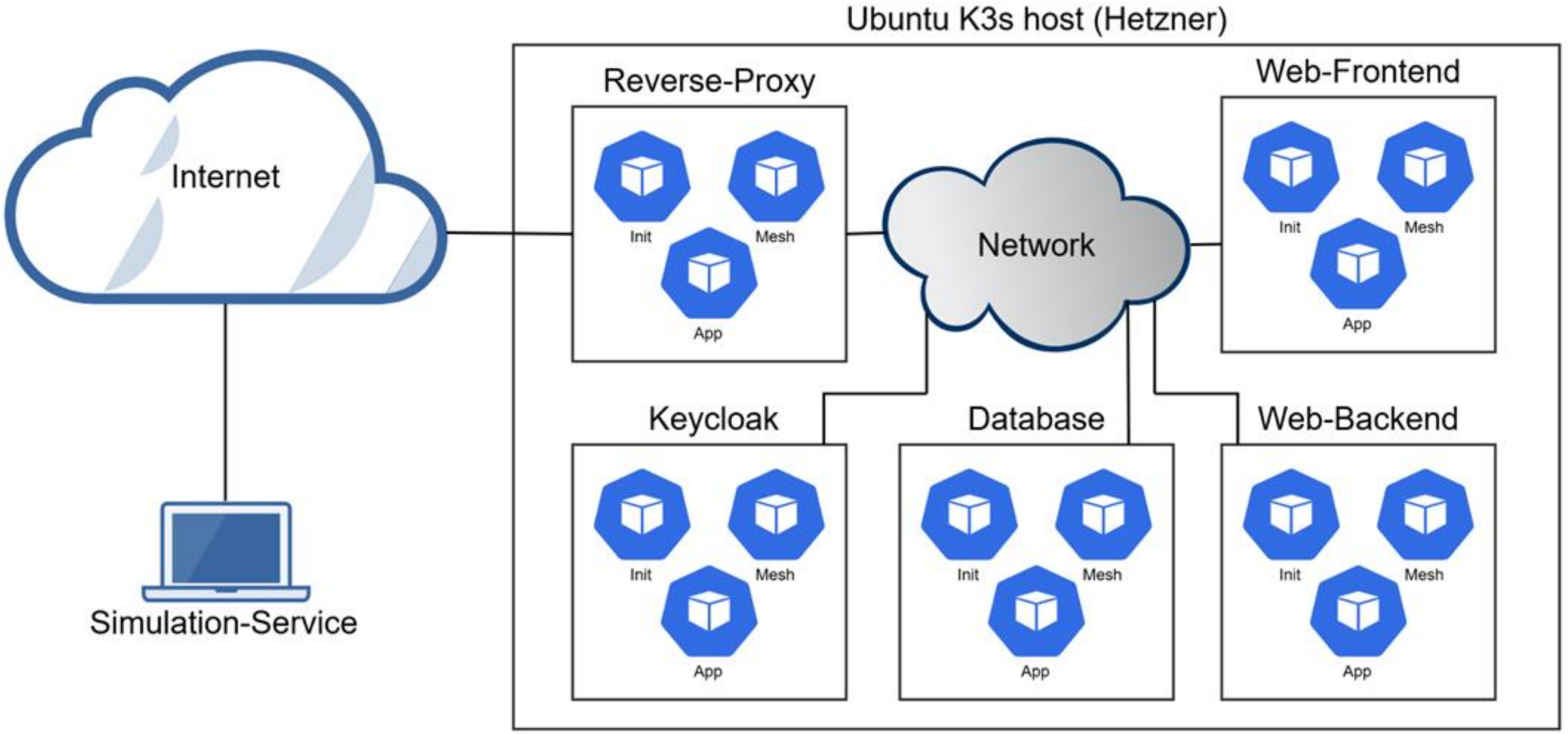
Migration steps from classic to confidential computing deployment

Existing configuration:

- Command and Control (C2) application
- contain:
  - Web application split over multiple containers
  - Frontend
  - Backend
  - Keycloak
  - DB

- Use volumemounts without subpath
  - Limit by kata containers
- Adapted the interconnection between the container
  - Mesh with mtls between the container
- Use own reverse proxy and not ingress controller
  - ingress controller is not secured by contrast
- Set limits for memory
  - Include the container image size
  - Needed ram for the running service

Demonstrator architecture overview



AIRBUS

Way forward Airbus DS on confidential computing study

01 **OC3: Proof of concept**
Fog (on-premises)

02 AFCEA: Initial Operational capability (IOC)
Cyber resilience check

03 Joint Artillery use case (including air gap, edge aspects)

04 Multi Domain Operation (MDO) use case
IaaS, Sovereign CSP

OC3 POC Target conclusion

- ✓ Ready for cyber resilience testing.
- ✓ Containerised application is functioning with Contrast.
- ✓ Information exchange function on top (data management) not affected.

AFCEA Target (IOC)

- Integration platform staged at ADS.
- More nodes simulated / interfaced in sandbox mode.
- Cyber resilience test conducted.
- Massive intelligence feasibility validated.

Special thanks to contributors
EDGELESS SYSTEMS: Thomas Strottner, Markus Rudy
AIRBUS DS: Holger Fritz, Ingo Schwarz, Mario Jähnert

Thank you