

ICEYE

Europe's EO Architecture

Design Principles from Operational ISR

May 2026

Europe's EO Architecture: Design Principles from Operational ISR

Executive summary

Four design principles from operational European ISR systems should ground the ERS and EOGS architecture: use federation to orchestrate systems running today and tomorrow; make security and speed structural design drivers from day one; specify stable and interoperable interfaces as top-level requirements; and design for incremental deployment and improvement.

Europe already operates systems that demonstrate all four principles. The work is connecting them, not building from scratch.

The architecture opportunity

Russia's invasion of Ukraine and Europe's climate-driven disasters have proven the same point: timely situational awareness is now a first-order security requirement. Defence, civil security, crisis response and strategic monitoring all need the same information. What differs is the tempo, security level, and degree of detail needed. Space-based EO is the one capability that delivers across all of them.

Europe has the asset base to meet this demand with approximately 150 to 250 satellites spanning Copernicus Sentinels and Contributing Missions, national governmental systems, and European commercial constellations. What does not yet exist is the federated architecture connecting them. One where defence and civil security users get assured access, guaranteed timeliness and priority during escalation, regardless of which asset provides the observation.

The ERS programme and the longer-term EU governmental EO architecture under the next MFF are the vehicles for building this. Both face a design choice that will determine their operational value: ground the architecture in systems already running in Europe, or in theoretical models of how a federated architecture might behave.

The four principles introduced here come from sovereign ISR systems that European armed forces and civil protection agencies operate today across seven nations, end-to-end. They reflect lessons from active conflict support, disaster response and peacetime monitoring, validated by continuous feedback from operational user communities.

Principle 1: Use federation to orchestrate capacity in systems running today and tomorrow

A federated EO architecture has to answer questions that individual national missions cannot: how tasking conflicts are resolved when multiple users request the same asset over the same area; who decides how capacity is allocated; how priority is set during a crisis; how service levels hold under peak load; how heterogeneous assets appear as a single system to users operating at tactical timelines. These are operational questions, and they have operational answers only when the federation is built on systems already in service.

Europe has those systems today. The Copernicus Data Space Ecosystem federates Sentinels and Contributing Missions for over 640,000 users through a single open-access platform. The ESA Copernicus Integrator Service federates across Contributing Missions. National dual-use SAR programmes operate civil and defence access on the same assets through distinct controls. NATO has integrated commercial SAR and optical assets into governmental service-level agreements. Each addresses a different part of the federation challenge under real operating conditions.

EOGS service-level design, governance rules, priority logic and interface contracts should be derived from the operational behavior of these systems, not from theoretical models. Where federated systems already work in Europe, EOGS should adopt the patterns that work. Where they reveal limitations, EOGS should design around those limitations using evidence rather than assumption.

The same evidence applies to the service level target. The federated systems running in Europe today operate across a wide range: civil platforms at hourly to daily cadence, sovereign defence platforms at tactical timelines. A federation built for 24-hour delivery is a fundamentally different problem from one built for 30-minute tactical delivery. Defence users need the latter. EOGS must be designed for that target from the start.

Principle 2: Make security and speed structural design drivers from day one

Security determines how a dual-use system is partitioned: which components share infrastructure, which require physical separation, where data crosses classification boundaries, and how tasking authority is delegated.

A governmental EO service must operate across multiple classification levels and multiple member state legal frameworks at once. Each combination imposes different constraints on ground segment topology, data routing, personnel clearance and cross-border interoperability. Defining these constraints alongside the functional architecture is the

only way accreditation can proceed in parallel with system development, at the speed and scale that operational needs today demand, rather than as a downstream gate that delays operational capability.

Security and classification rules must shape how the system is broken into components from the start, not be added once components are already designed. At the same time, the trade-off between security and tactical performance is real and must be considered from day one. This is what makes accreditation-ready design for strategic, tactical and commercial operations possible across multiple classification levels and member state legal frameworks.

Principle 3: Specify stable, interoperable interfaces

Two conditions apply: the interface contracts must be specified as top-level architecture requirements, and the interfaces must be open to all qualified assets across vendors and sensors.

Interface contracts can be defined up front through specification, or they can emerge de facto through implementation. Both paths produce working architectures. What matters for EOGS is that whoever holds the interface, by specification or by de facto adoption, opens it to other qualified contributors. Where this does not happen, an end-to-end system cannot be put together from different vendors and sources, and participation in a system Europe collectively funds depends on negotiated access.

If the interfaces are not open to all qualified assets, the architecture cannot absorb new sensors, new providers or new member state contributions without bespoke integration work each time. Lack of interoperability mainly limits speed and performance.

The operational evidence for getting both conditions right is European and available today. Multiple nations operating sovereign SAR constellations are building toward federated capacity management at tactical timelines through a shared orchestration layer, where fleet-level capacity is visible across partners while tasking execution and data authority remain under strict national command. Finland, Sweden, Poland and the Netherlands are actively developing this cross-tasking capability using systems already deployed for their sovereign missions to boost national capacity and, when needed, engage in joint operations or reach tactical timelines. On the civil side, over 640,000 users access multi-source data through the Copernicus Data Space Ecosystem, federated through interface contracts that allow heterogeneous national and commercial assets to appear as a single system.

The federation layer specification must be the first requirement fixed, not the last. It is the most important top-level requirement, and the one that determines whether the architecture can evolve as one European system or be constrained and fragmented by its initial implementation and participants.

Principle 4: Design for incremental deployment and improvement

An EOGS architecture must be scalable-by-design and component-replaceable, not monolithic. Sensors, transport layers, data platform and processing must be upgradeable or scalable independently, as technology and mission needs evolve over time.

Sovereign SAR satellites now go from contract signature to launch within twelve months, and platform generations refresh every one to two years. Software-defined space systems receive regular software upgrades that contribute significant capability improvements over their lifetime. This is the technology cadence EOGS must accommodate to stay current over its service life.

This is only possible when each layer has an independent upgrade cycle. Space segment evolution does not force ground segment redesign. Ground segment upgrades do not require satellite replacement. Analytics can be added or replaced without touching either.

A monolithic architecture pays its cost up front and locks in the technology of the day, a model that worked when most innovation came from hardware. Software-driven systems require a modular, component-replaceable architecture that absorbs continuous innovation across its lifetime, with a cost-benefit ratio that improves over the system's operational life.

EOGS must deliver first operational capability within the political mandate window and continue serving users for decades. The choice is between delivering early and evolving continuously, or waiting for full readiness and depreciating from day one.

Design principles summary

- Federate to orchestrate capacity across systems running today and tomorrow. Derive EOGS service levels, governance and interface contracts from European federated systems already in service.
- Make security and speed structural design drivers from day one. Classification rules must shape system decomposition from the start, so accreditation runs in parallel with development at tactical timelines.
- Specify stable, interoperable interfaces as top-level requirements. Interface contracts defined up front and open to all qualified assets let the architecture evolve as one European system.
- Design for incremental deployment and improvement. Modular, component-replaceable architectures deliver first operational capability within the political mandate window and absorb continuous innovation across decades.

These principles are derived from sovereign ISR systems operational across seven European nations, shaped by continuous user dialogue under real conditions, including active conflict and large-scale disaster response.