Quality Versus Complexity (The Galileo Product Assurance Experience)

TRISMAC CONFERENCE 16th April 2008

Presentation by:

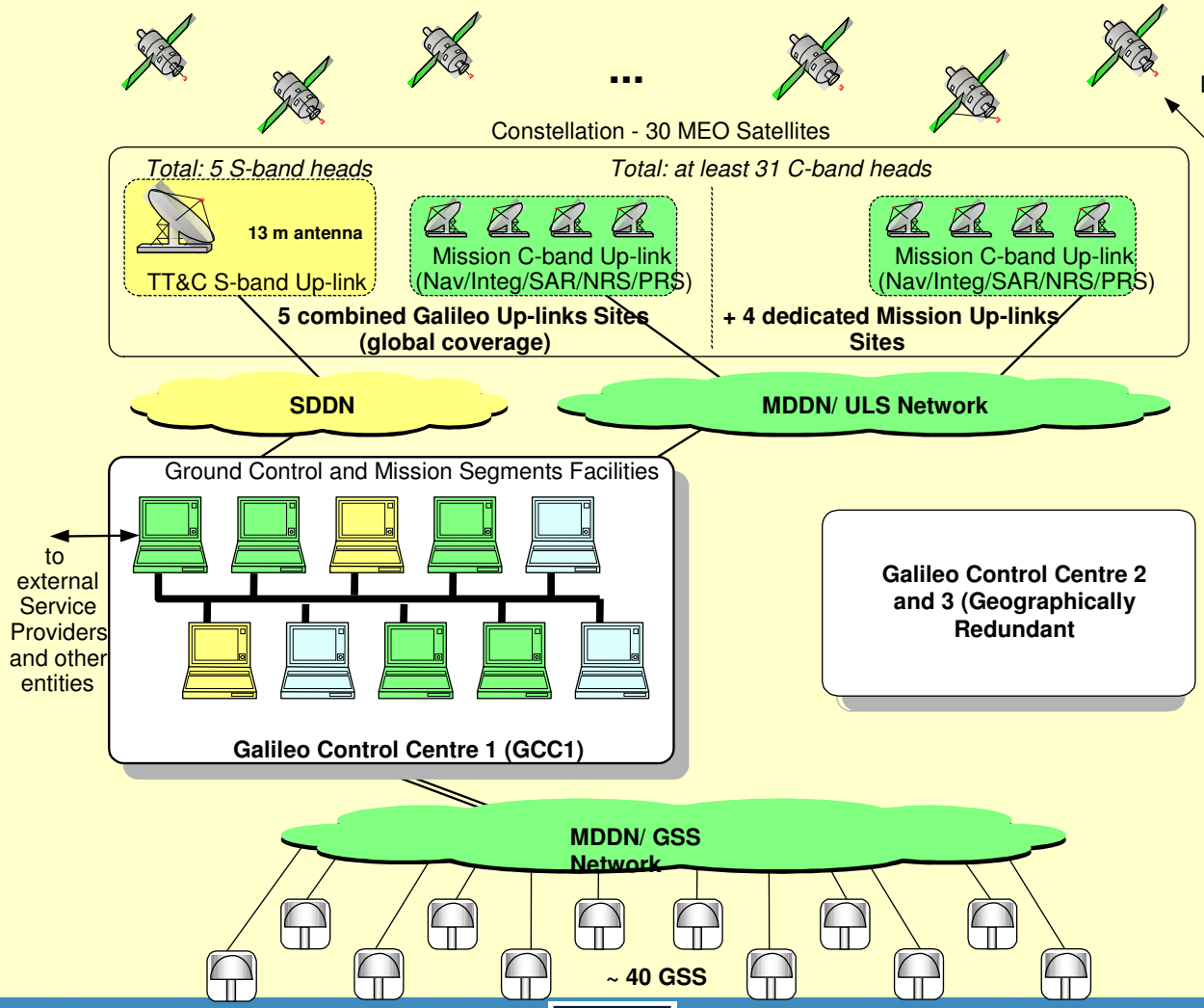
Nigel Watts

Head of Galileo Product Assurance and Safety Office

Introduction

- A simple product built by 1 man can be of the highest quality if he is skilled and knows how to make it. Complex Quality Standards aren't relevant.
- An equipment box for a Satellite needs to be built to stringent requirements including quality and needs to be verified and documented to conform to requirements.
- Applying and implementing standards like the ECSS to such equipment or furthermore to one or a few satellites makes sense; they contain a wealth of knowledge based on many years of experience to help ensure a conformant end product.
- What about Galileo?

Overall Architecture - Physical View



ERIS - External Regional Integrity Systems

GCS - Galileo Control System

GMS - Galileo Mission System

GSS - Galileo Sensor Stations

MDDN - Mission Data Dissemination Network

NRS - Navigation Related Service

PRS - Public Regulated Service

SAR - Search And Rescue

SDDN - Satallite Data Dissemination Network

TT&C - Telemetry, Tracking and Telecommand

ULS - Up-Link Station

Elements of GCS and GMS

Elements of GMS

Elements of GCS

GALILEO Services

- **Open Service**
  - Mass-Market applications not requiring any guarantee.
  - As accurate as conventional differential GPS but without requiring additional ground infrastructure.
    - Horizontal Accuracy: 4 meters, 95% confidence
    - Vertical Accuracy: 8 meters, 95% confidence
- **Safety of Life Service:**
  - Guaranteed service for Safety-of-Life applications
  - Integrity Alerts
- **Commercial Service:**
  - Professional use and guaranteed service in return for a fee
  - System capabilities introduced to foster application with commercial interest (additional navigation signals, low-data rate broadcasting capacity).

GALILEO Services (cont'd)

- **Public Regulated Service:**
  - Police, coast guards, customs, strategic civil infrastructure…
  - High continuity of service.
  - Signals more robust to interference.
  - Access to the service to government authorized-users only.
- **Search and Rescue Service:**
  - Relay of distress alarms to improve existing relief and rescue services.
  - Compatible with COSPAS-SARSAT

GIOVE A

- Risk Minimisation rather than Risk Elimination
- ECSS were used mostly as guidelines or not followed at all.
- In House Design Manufacturing and Testing
- Few Subcontractors
- Mix of Commercial (with heritage) and Space Qualified Components
- RAMS analysis positively influenced the design
- Poor documentation and almost non existent End Item Data Package
- Design allowing for significant parallel integration and testing
- Delegated PA Responsibility to Engineering
- Dedicated PA Manager after CDR

GIOVE B

- ECSS fully applicable with tailoring
- Higher Quality Components (space qualified)
- RAMS after the fact
- Contractual difficulties
- Lengthy delays
- Cost overruns
- Extensive documentation
- Launch campaign now on track for launch early on 27th April 2008.

In Orbit Validation Project

- 4 Satellites and Main Ground Infrastructure to allow validation of Major System requirements

Main Principles for PA on the Project:

- ECSS for Space Segment with some Tailoring
- ECSS and other Sources heavily tailored for Ground Segment
- Software Standard Developed based on ECSS and DO 178B
- Automated Tools used where possible:
  - Non Conformance Tracking System
  - Galileo Software Tracking Tool
  - DOORS for Traceability and Verification Database
- Dedicated EEE Requirements Specification
  - ECSS level B components Quality
  - Self Procurement allowed
  - Non Standard Parts approved via Parts Control Board
- Security Accreditation placed in PA Domain

In Orbit Validation Project (cont.)

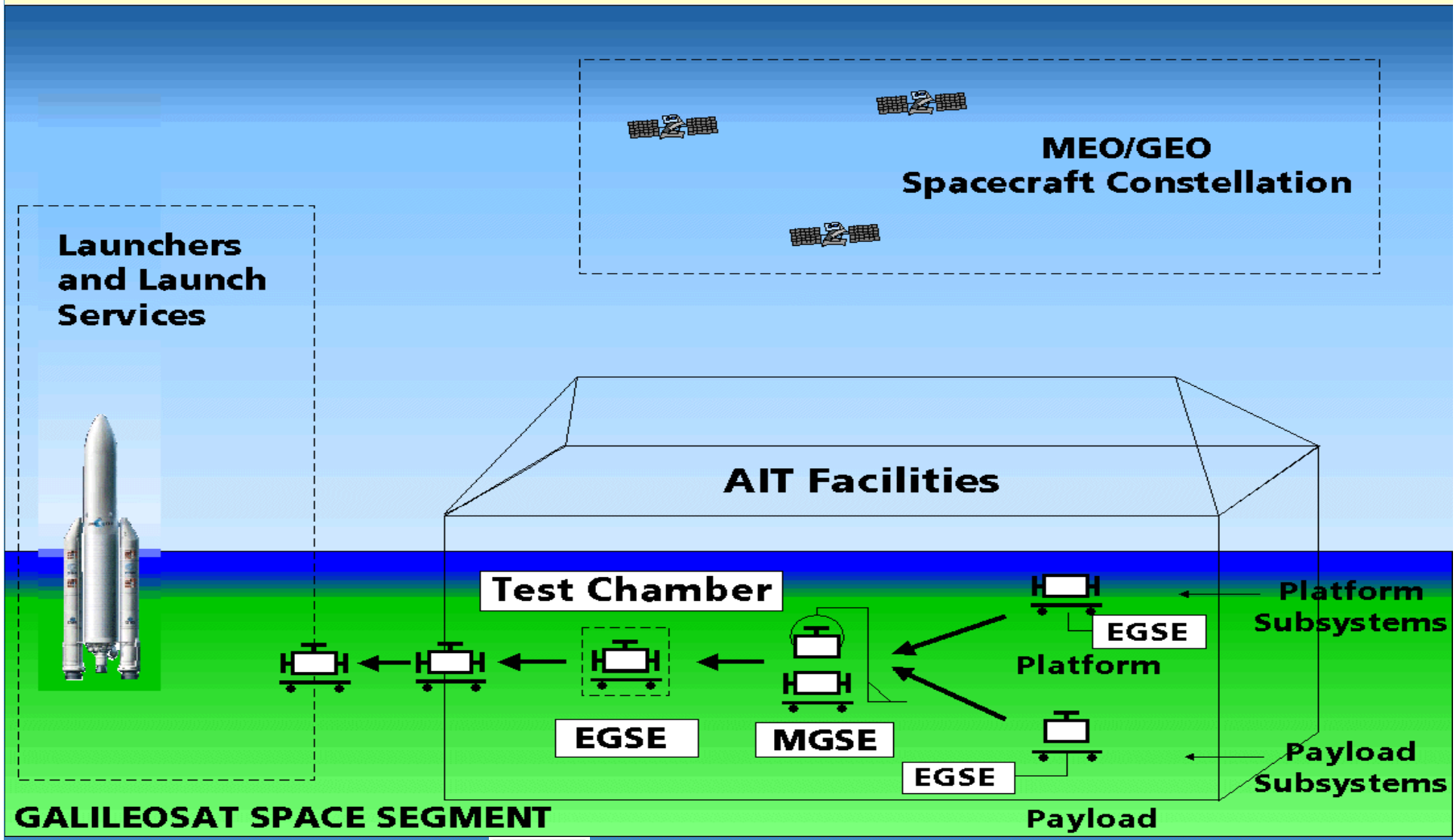
Problems encountered:

- Large Complex Industrial Organisation with overall Prime inefficient
- Conflicting National Security Interests
- Difficulty to Freeze baseline
- Contract with Prime terminated end 2007/early 2008.
  - ESA now acting as Prime Contractor under EC
- Significant De-Scoping

Full Operational Configuration

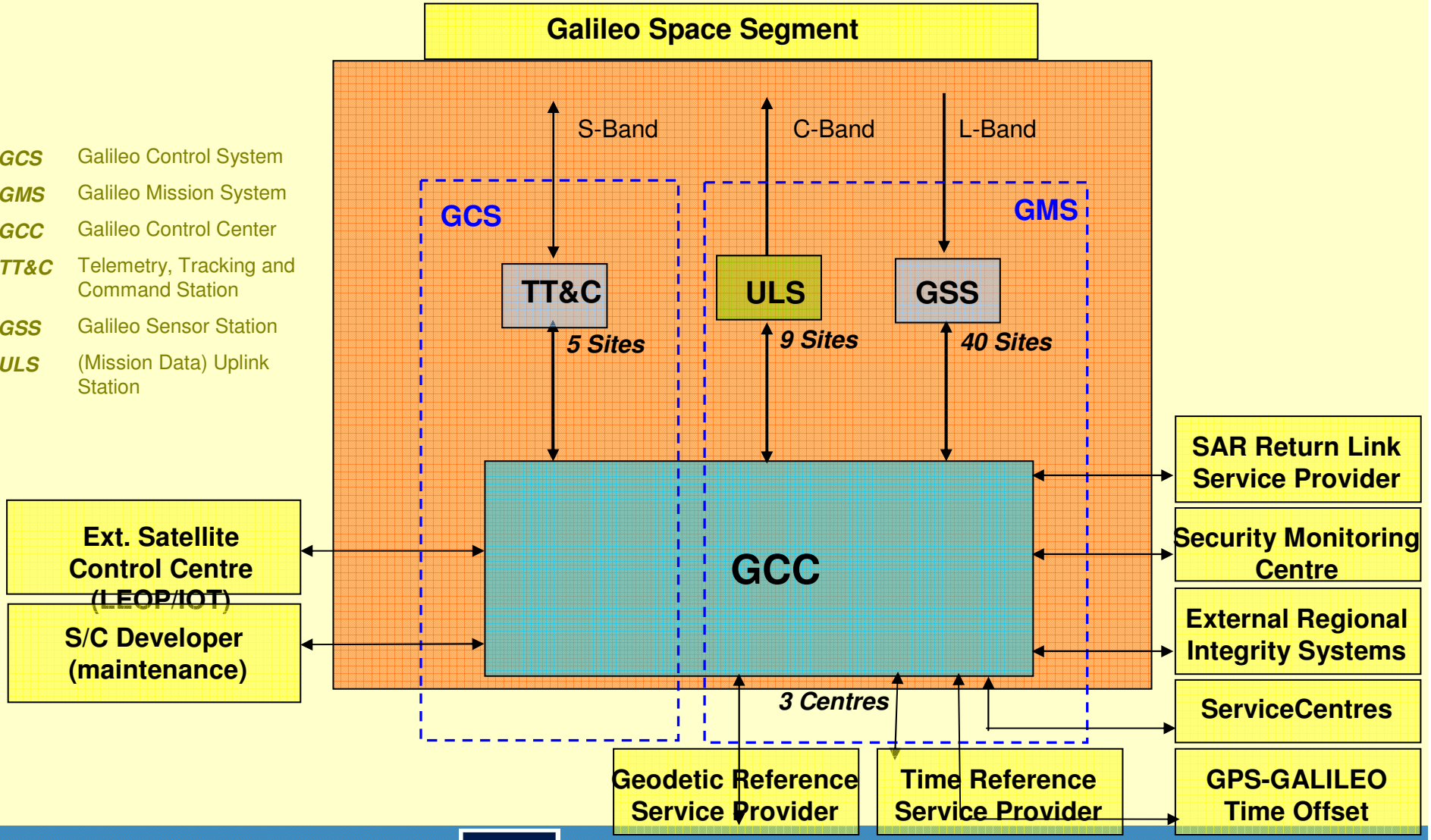
- Individual Satellites are not Mission Critical
  - Can we relax some requirements?
  - EEE Procurement Policy
  - Testing
  - Quality Assurance
- The Ground Segment is complex, heavily dependant on Software and some elements are Mission Critical.
  - Do we need extra Requirements?
- Re-Scoping
- Multiple Production
- Security Accreditation
- Certification

Space Segment - Overview

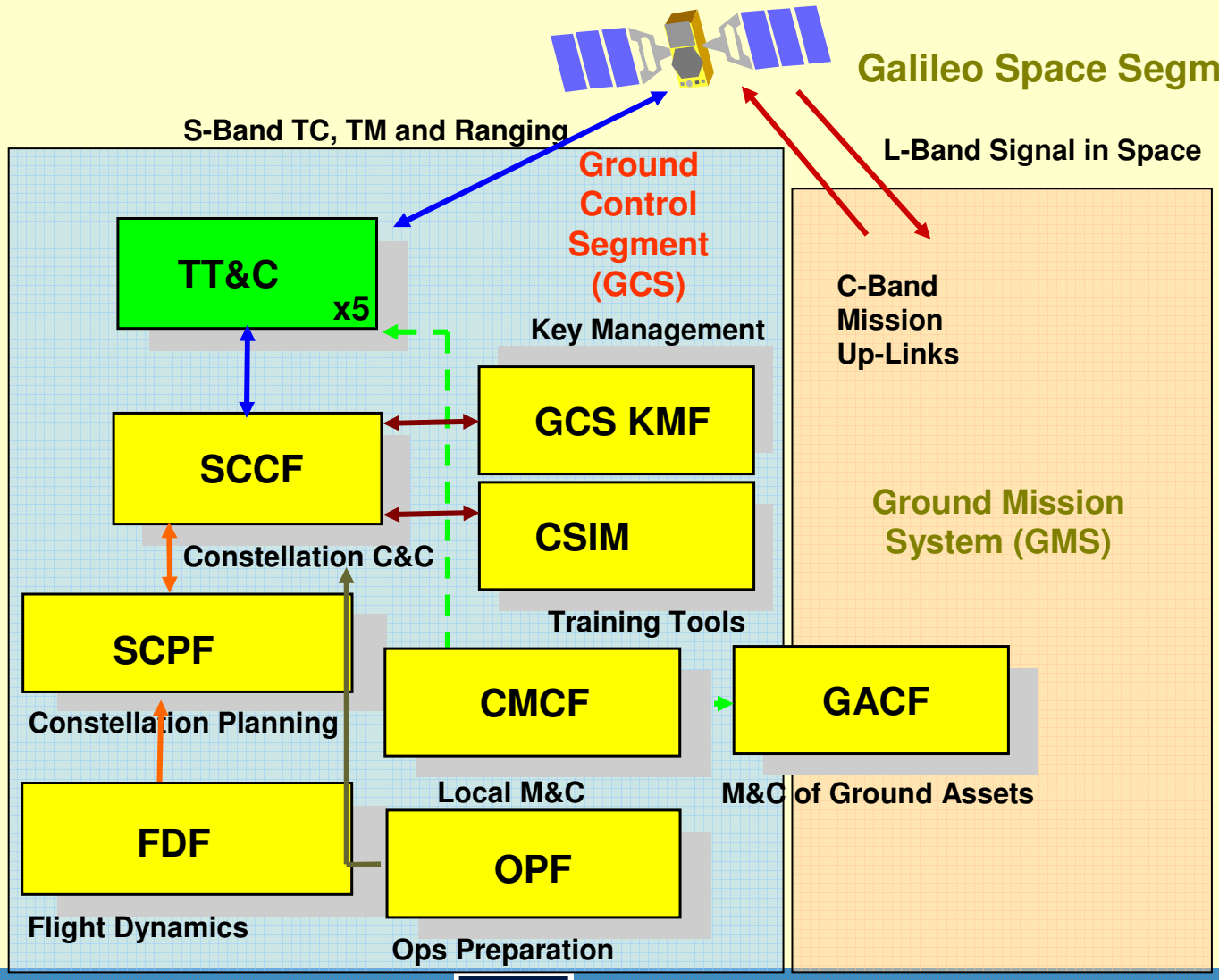


Ground Segment – Architecture & I/F

GCS	Galileo Control System
GMS	Galileo Mission System
GCC	Galileo Control Center
TT&C	Telemetry, Tracking and Command Station
GSS	Galileo Sensor Station
ULS	(Mission Data) Uplink Station

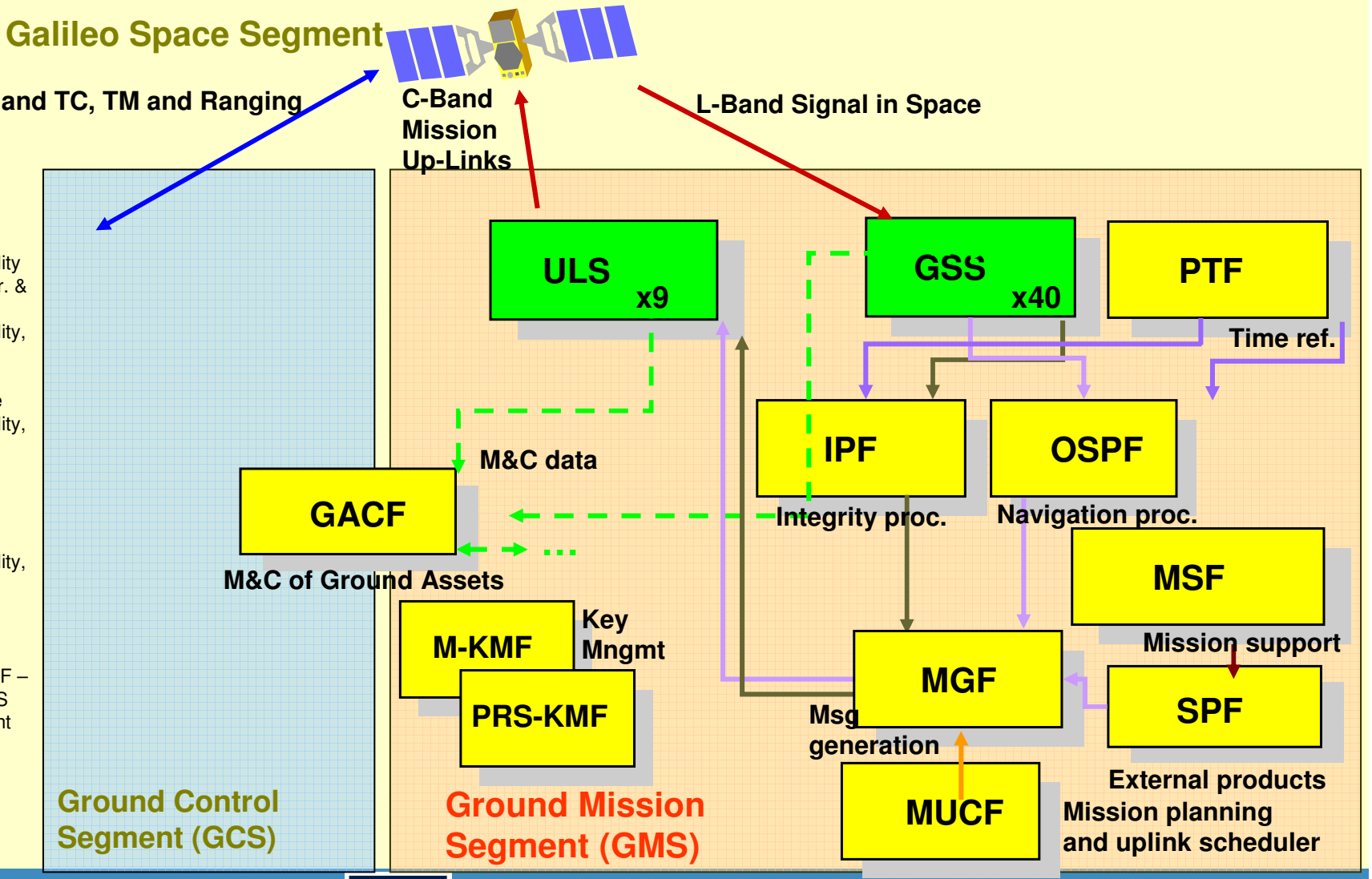


Ground Control Segment – Architecture



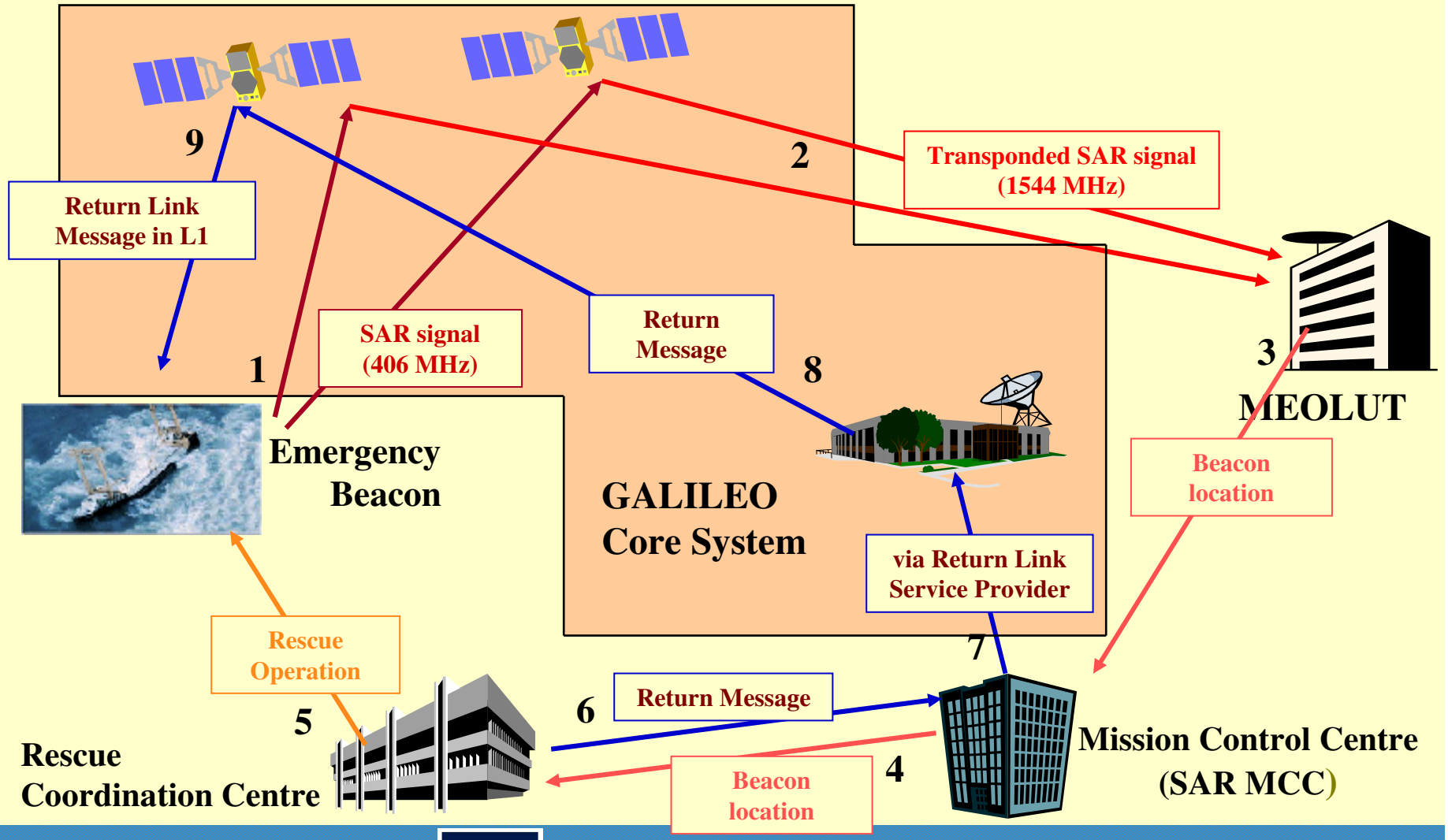
TTC – Telemetry Tracking and Control,
SCCF – S/C Constellation Control Facility,
SCPF – S/C Constellation Planning Facility,
FDF – Flight Dynamics Facility,
OPF – Operations Preparation Facility,
GACF – Ground Assets Control Facility
CMCF – Central Monitoring & Control Facility
GMS KMF – GMS Key Management Facility
CSIM – Constellation Simulator

Ground Mission Segment – Architecture



GSS - Galileo Sensor Station,
IPF – Integrity Processing Facility
OSPF – Orbitogr. & Synchronisation Processing Facility,
PTF – Precision Timing Facility,
MGF – Message Generation Facility,
ULS – Uplink Station,
MCF – Mission Control Facility,
ULF – Uplink Scheduling Facility,
MSF – Mission Support Facility,
SPF – Service Product Facility,
M- and PRS-KMF – Mission and PRS Key Management Facility,
GACF – Ground Assets Control Facility

SAR/Galileo Architecture



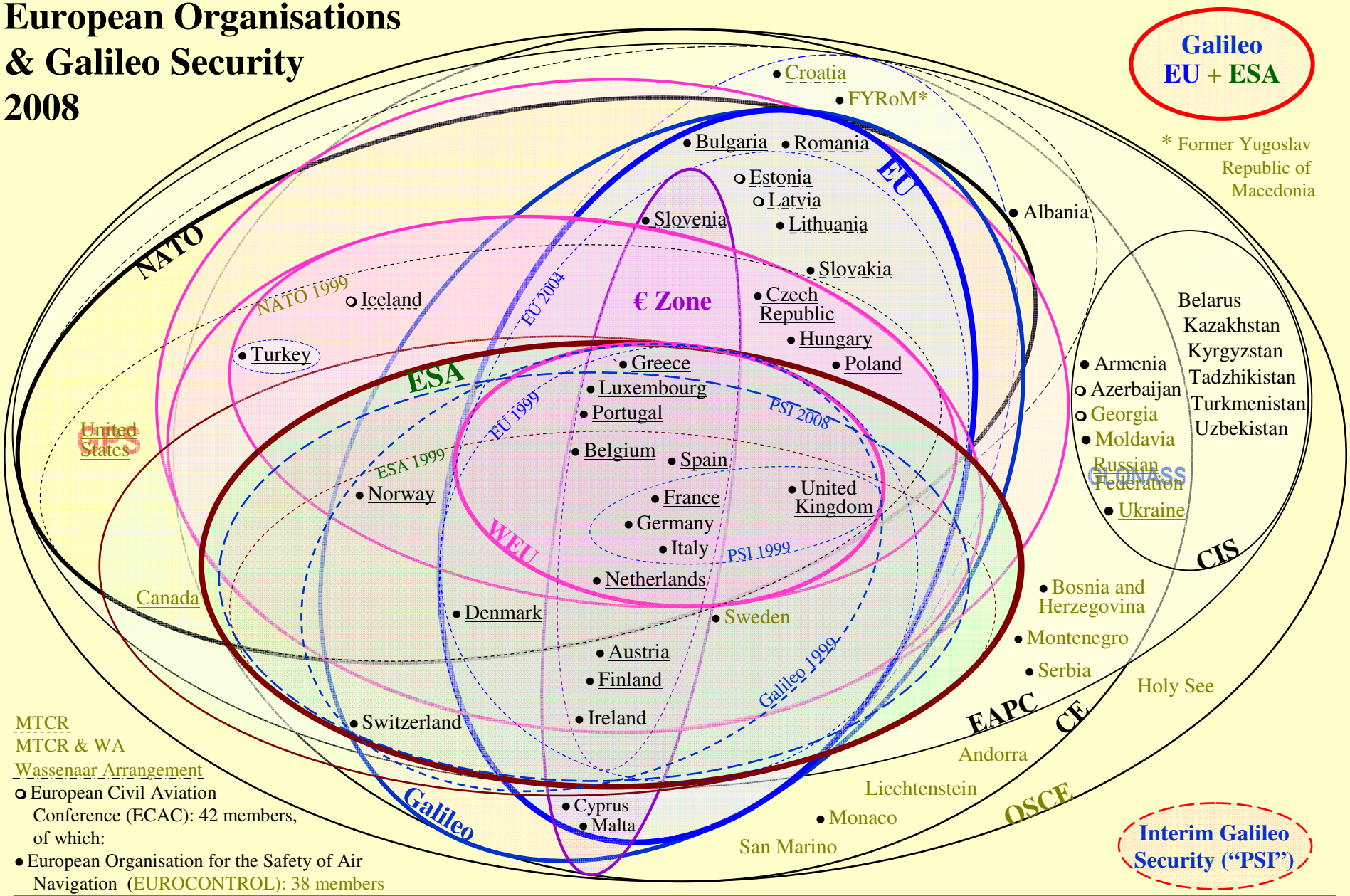
Conclusions

- Some costly redevelopments due to RFD's accepted for IOV
- High complexity and many interfaces especially in the security domain very challenging, indicating need for additional innovative quality efforts to minimise risk

Recommendations:

- Early frozen technical baseline
- Clean interfaces and management structure especially in the Security domain
- Balance requirements between
  - ECSS
  - Lessons from Industrial/Commercial programmes and organisations that build complex reliable systems at low cost
  - Mission requirements
  - Identified Risks
- PA Plans must demonstrate understanding of Galileo's special needs and the measures to address them:
  - "Dusting off" and re-labelling of old company PA Plans is unacceptable for Galileo
- Adjust to the challenges

European Organisations & Galileo Security 2008



OSCE: Organisation for Security and Cooperation in Europe: 56 members **EU**: European Union: 27 members + *3 candidates* **CE**: Council of Europe: 47 members
WEU: Western European Union: 10 members + 6 associates + 5 observers + 7 partners **NATO**: North Atlantic Treaty Organisation: 26 members + *3 candidates*
ESA: European Space Agency: 17 members + 1 co-operating State **EAPC**: Euro-Atlantic Partnership Council: 49 members
CIS: Commonwealth of Independent States: 12 members **€ Zone**: 13 members