ARTAS

What about our safety documentation?

Part 1

Regulation context

EC 482-2008

Article 1

Subject-matter and scope

1. This Regulation lays down the requirements for the definition and implementation of a software safety assurance system by air traffic service (ATS) providers, entities providing air traffic flow management (ATFM) and air space management (ASM) for general air traffic, and providers of communication, navigation and surveillance (CNS) services.

It identifies and adopts the mandatory provisions of the Eurocontrol Safety Regulatory Requirement — ESARR 6 — entitled 'Software in ATM Systems' issued on 6 November 2003.

2. This Regulation shall apply to the new software and to any changes to the software of the systems for ATS, ASM, ATFM, and CNS.

It shall not apply to the software of airborne constituents and to space-based equipment.

ANSP Safety Management Manual

- Shall include overall risk assessment and mitigation process
- ESARR6 & EC482/2008 make sense only if safety assessment was conducted
  (to get the SWAL meaning safety criticality of the Software)
- There must be a chapter dealing with software aspects in the SMS (reinforced in 1035/2011)

Summary

- EC 482/2008 – EC 1035/2011
- ANSP shall do an overall risk assessment and mitigation process
- Software Assurance Level ⇔ Software criticality

- What about our safety documentation?

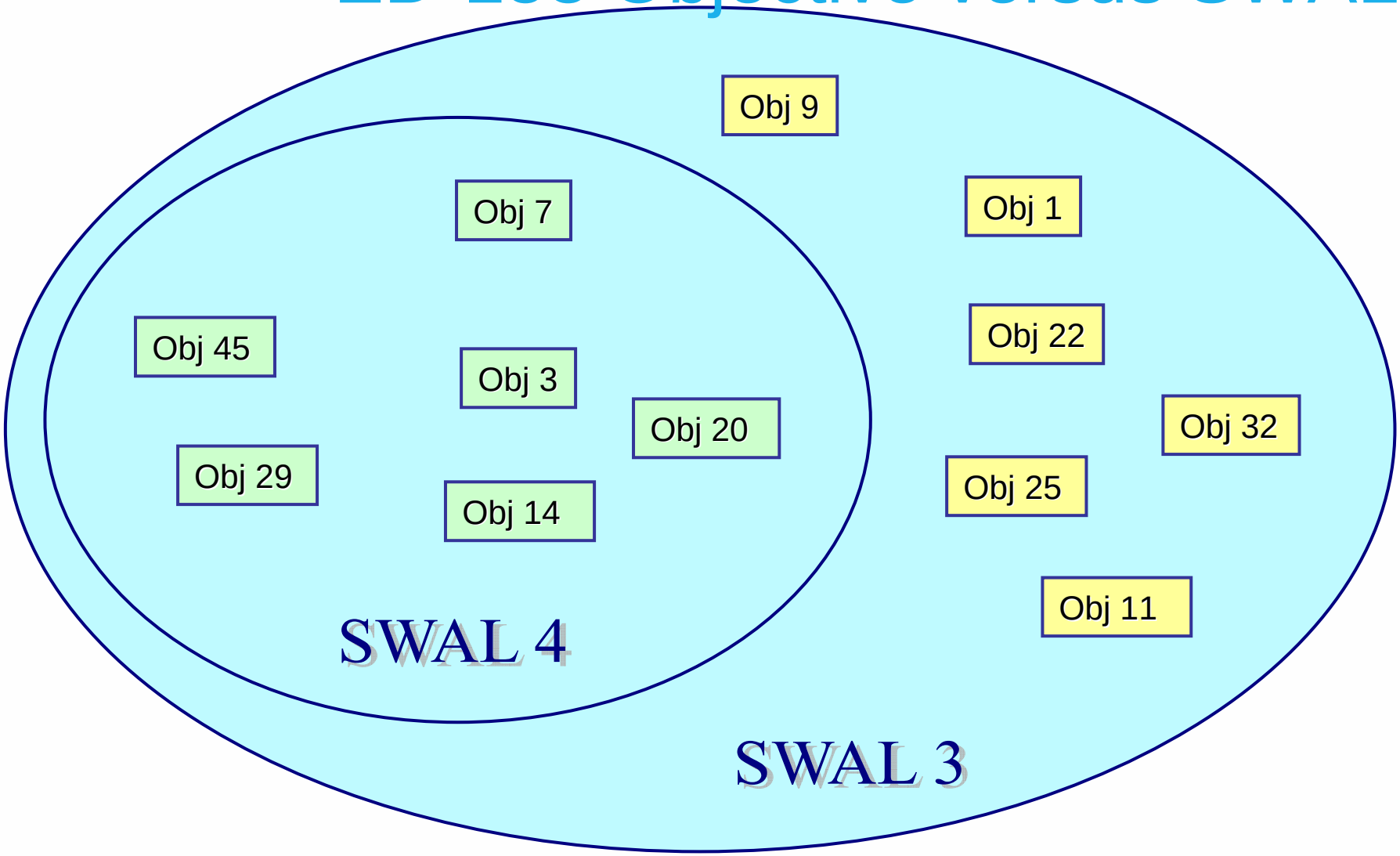
Part 2

Acceptable Means of Compliance

AMC

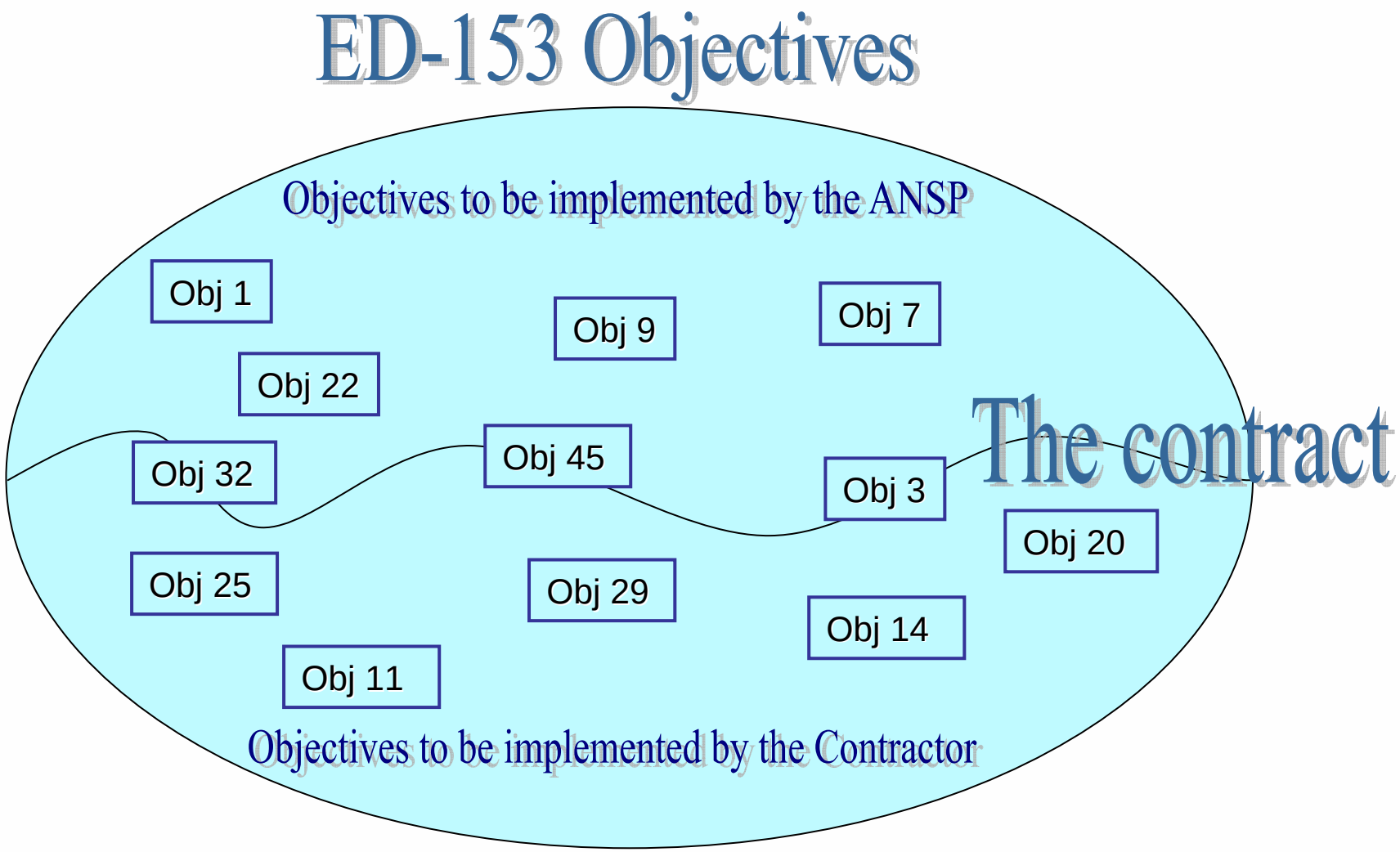
- Nothing today!
  But
- ED-153 (EN 16516 currently under review)
- ED-153 addresses the complete software lifecycle

ED-153 Objective versus SWAL



SWAL3 = SWAL 4 + SWAL 3 Specific Processes

ED-153 Objective Implementation



Summary

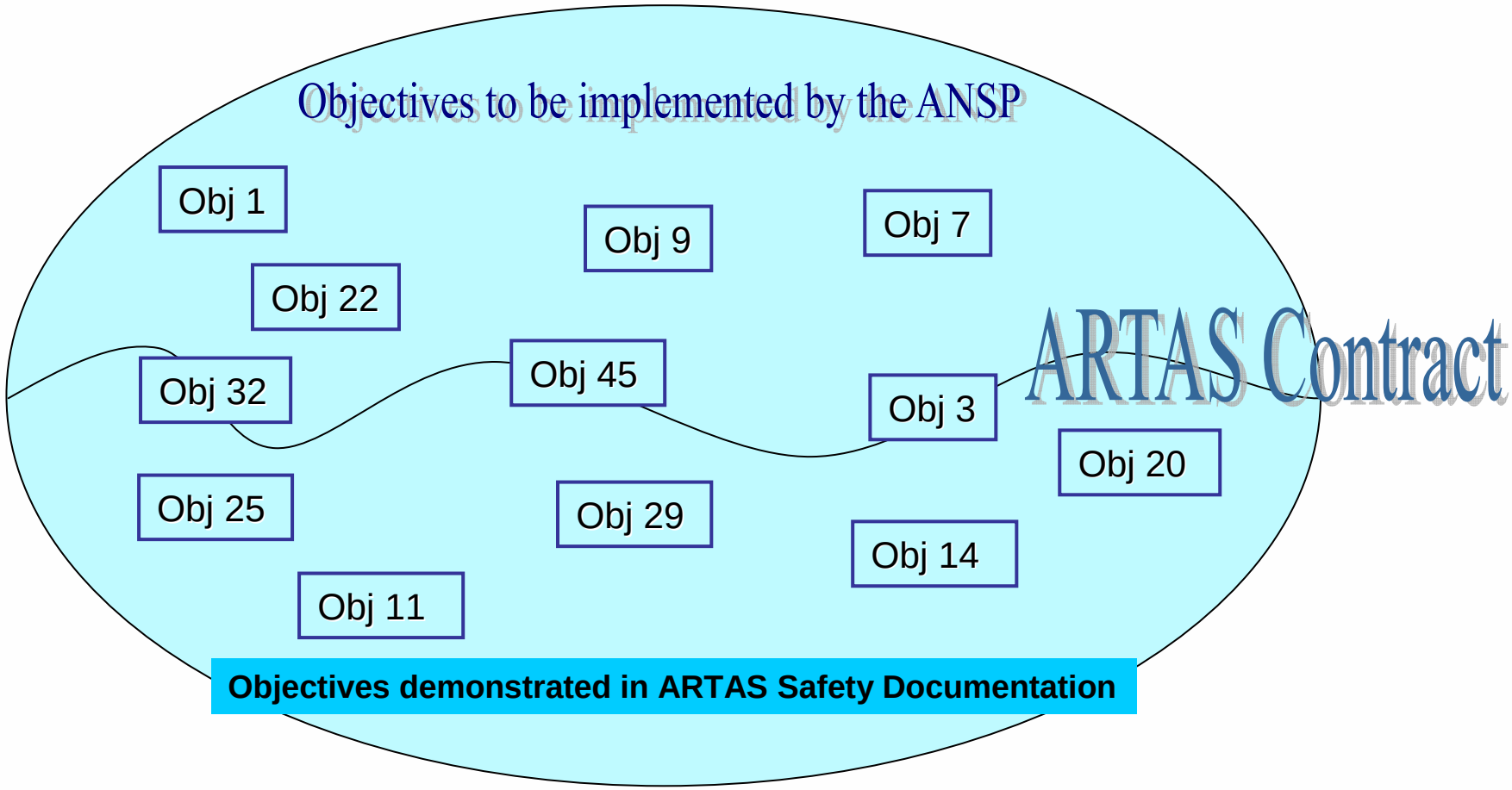
- SWAL identifies the objectives to be demonstrated by the ANSP
- Software can be contracted (COTS or new development)

- What about our safety documentation?

Part 3

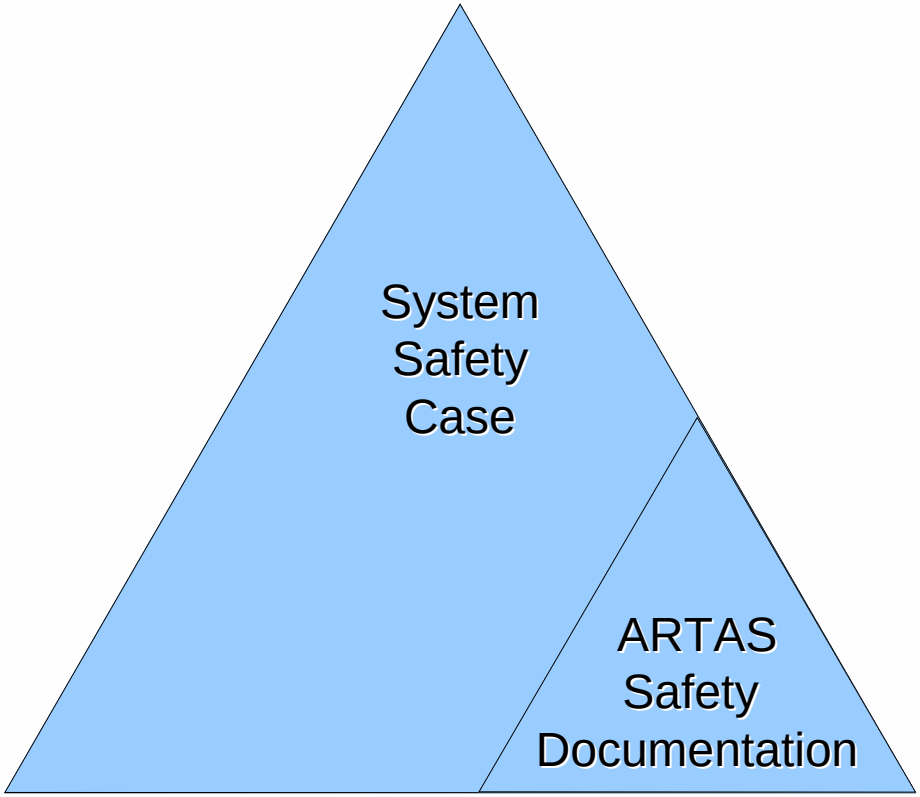
ARTAS Safety Folder Report

What about ARTAS safety documentation



ANSP safety argument

Simplistic view (over simplified)



Summary

- ARTAS comes with its SWAL3 Safety Folder Report
- This report enables ANSPs to demonstrate ARTAS up to a SWAL 3

- What about our safety documentation?

Part 4

Linking all together

What's in?

- All required evidence that ARTAS was developed according to SWAL 3 set of objectives
- Example 1:
  - 5.2.1 Configuration Management Process Implementation
    Evidence:
    - The CAMOS Configuration Management Plan has been produced to cover those salient points above.

    Documentation:
    - CAMOS Configuration Management Plan (CMP).

What's in?

- Example 2:
  - 4.3.5 Software Architectural Design
    Evidence:
    - Software Architectural Design documents for all ARTAS CSCIs have been created.

      ….

    Documentation:
    - The following Software Design Descriptions (SDD) are available:
      - ARTAS-ACOM-SDD
      - ARTAS-DAF-SDD
      - ….

What's missing

- Instantiation in your context:
  - FHA, PSSA, SSA in ANSP's environment,
  - The complete safety argument.

- Examples:
  - Transfer into operation is acceptably safe,
  - Operation and maintenance processes are acceptably safe…

Summary

- About our safety documentation:
  - ARTAS comes with generic partial safety argument.
  - Within the scope of the ANSP SMS & Software Safety Management System the ANSP shall instantiate and complete the ARTAS Safety Folder Report.

Questions?