SOFTWARE SAFETY WORKSHOP AND ES² SOFTWARE WORKSHOP

IDS Lessons Learned in European and Overseas Scenarios

Paolo Stefani
*Air Navigation System Engineering Director*

*Christian Visani*
Safety & Regulatory Compliance Manager

Luxembourg May 07-08, 2013

EC Reg. 482/2008 Vs IDS Software Products

ANS — *EC Reg. 549/2004 Art.2(4)*

EC Reg. 482/2008 Art. 1(1)

ATFM	ASM	ATS		CNS	MET	AIS

EC Reg. 549/2004 Art.2(11)

FIS	ALS	ADS	ATC

EATMN — *EC Reg. 549/2004 Art.2(17) (EC Reg. 552/2004 Annex I)*

ATM — *EC Reg. 549/2004 Art.2(10)*

Scope of ED-153 — *EUROCAE ED-153 Chap. 1.1 prEN 16154:2010 Chap. 1*
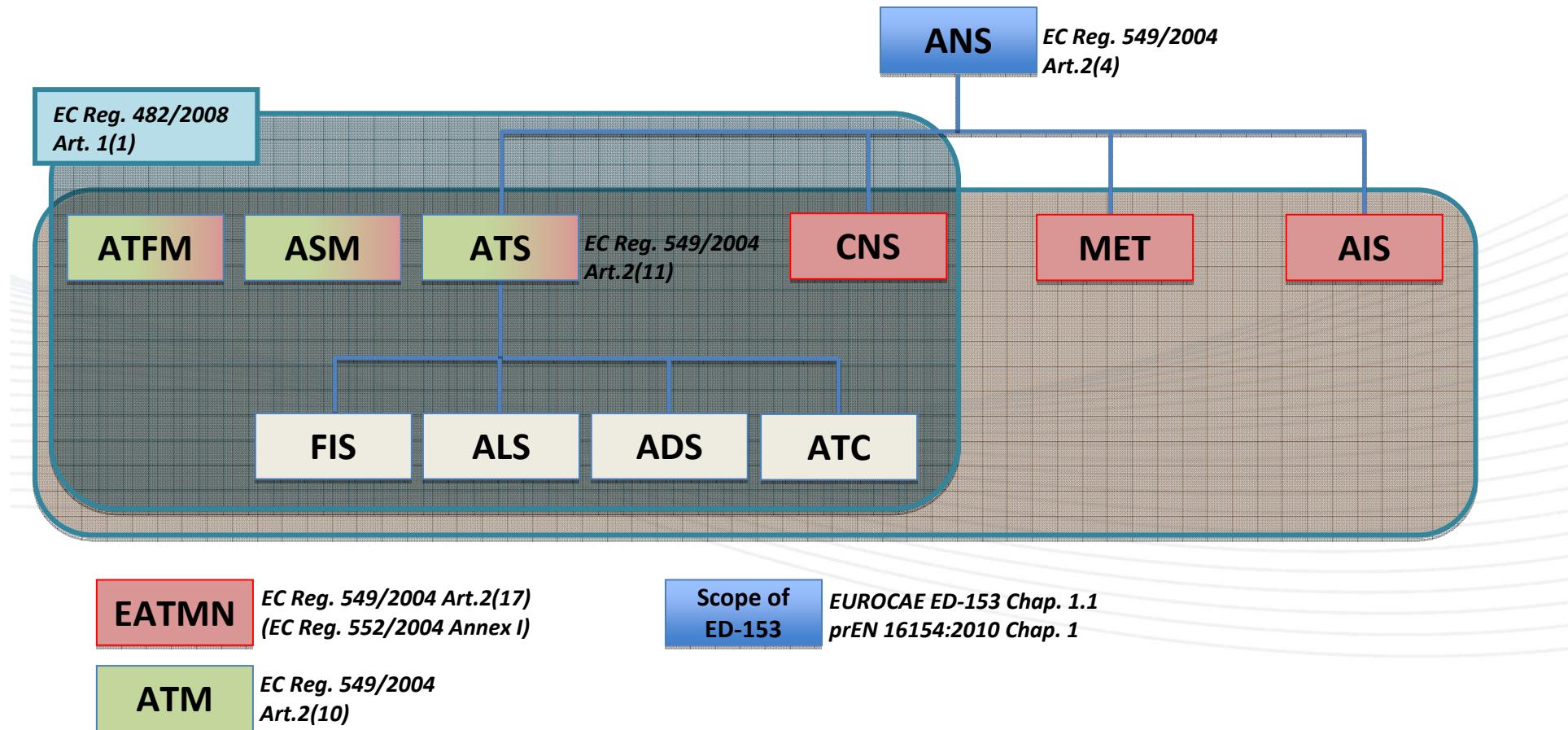
Impact on IDS-SpA Software Products

➢ Several discussions with Major European ANSPs (Operational and R&D Projects);

➢ Identification of the IDS SW Products that need to comply with ED-153 Objectives;

IDS SW Products → Within the framework of Reg. 482 → Mostly in line with ED-153 / Far from ED-153 Objectives

IDS SW Products → Not within the framework of Reg. 482

Series of multiple questions...

...involving all the IDS Air Navigation Division, Laboratories and Q&S Department...

...involving major IDS customers (including not European).
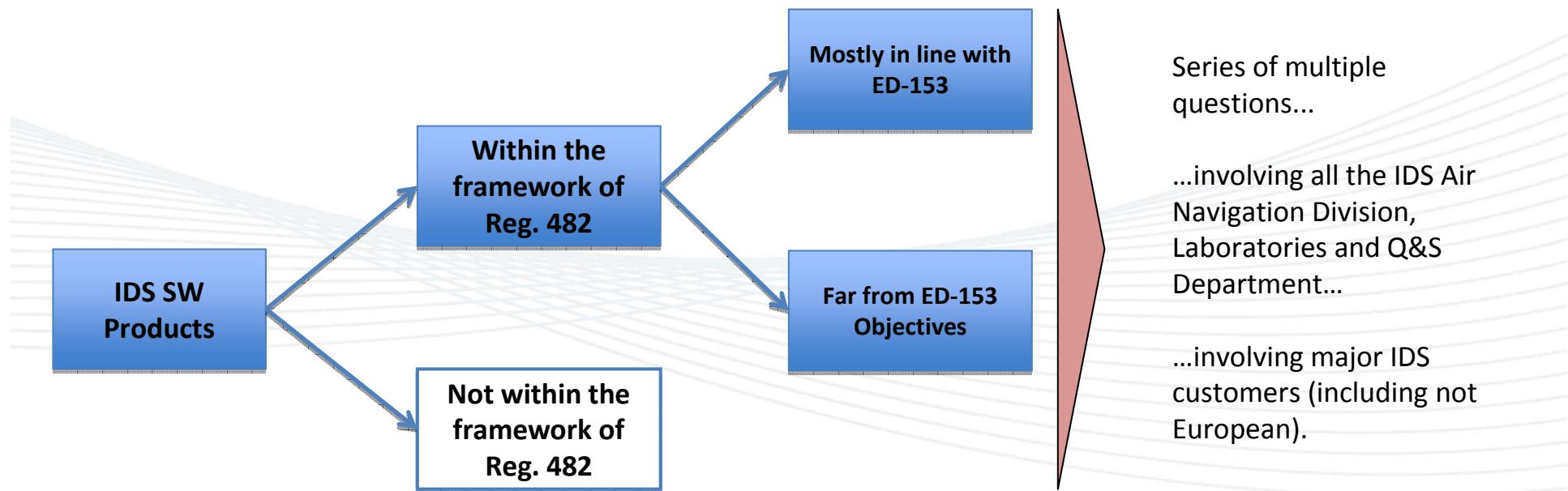
SW Assurance Allocation Matrix and required evidences

Sev. \ Lik.	1	2	3	4
V.P.	SWAL 1	SWAL 2	SWAL 3	SWAL 4
P.	SWAL 2	SWAL 3	SWAL 4	SWAL 4
V.U.	SWAL 3	SWAL 4	SWAL 4	SWAL 4
E.U.	SWAL 4	SWAL 4	SWAL 4	SWAL 4

Relaxing →

Sev \ Lik.	1	2	3	4
V.P.	SWAL 1	SWAL 2	SWAL 3	SWAL 4
P.	SWAL 2	SWAL 3	SWAL 3	SWAL 4
V.U.	SWAL 3	SWAL 3	SWAL 4	SWAL 4
E.U.	SWAL 4	SWAL 4	SWAL 4	SWAL 4

Standard ED-153 SWAL Allocation Matrix

Tighter →

Sev. \ Lik.	1	2	3	4	5
V.P.	SWAL 1	SWAL 2	SWAL 3	SWAL 3	SWAL 4
P.	SWAL 2	SWAL 3	SWAL 3	SWAL 3	SWAL 4
V.U.	SWAL 3	SWAL 3	SWAL 3	SWAL 4	SWAL 4
E.U.	SWAL 4	SWAL 4	SWAL 4	SWAL 4	SWAL 4

Approach for SWAL Level Allocation and ED-153 Objective Application

➢ First tentative SWAL allocation for AIS Software Products in 2009, considering:

   ✓ Safety Analysis developed with one of the major European ANSP;

   ✓ Feedback from customer with SW into operation;

   ✓ Business opportunity (Competitors statements).

➢ Management of "Previously Developed SW", "Development" and "COTS":

SW lifecycle evidences provided to customer when ad-hoc development required by contract

COTS: Lifecycle data defined by the contract
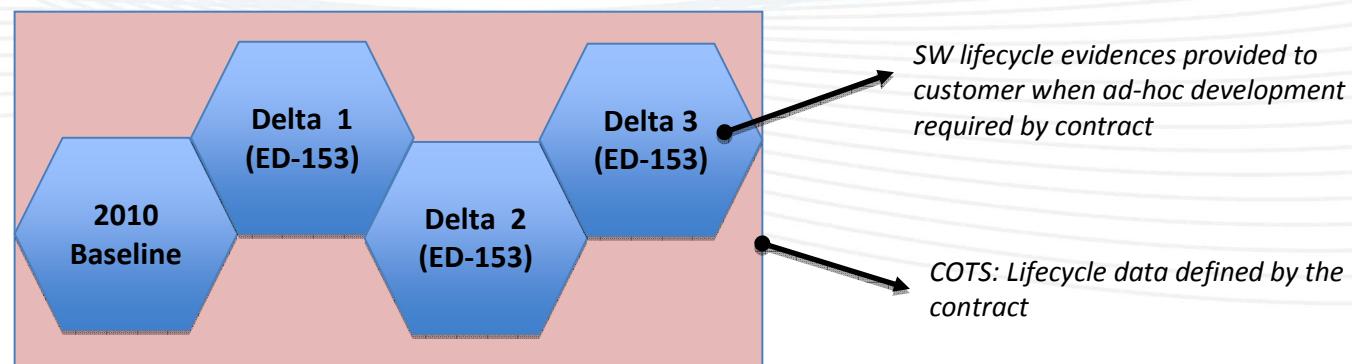
SWAL Allocation impact on IDS SW Lifecycle

Regulatory/International
Standard Requirements

Customer
Requirements

IDS Internal
Requirements

SW
Life
cycle
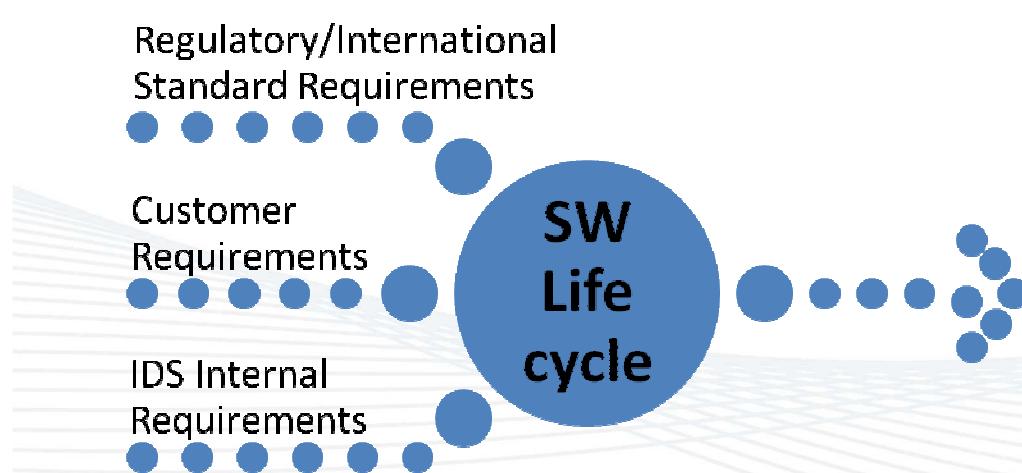
Update/modification to the IDS SW Lifecycle
Operating Instruction:

➢Initial Top-Down approach;

➢Improvements by a Bottom-Up approach;

➢SW Lifecycle tailoring in the SW Development
Plans;

➢Toward a scalable SW Development and
Verification Process (Considering Customers
Requirements and based on application of DO-
178 experience);

➢«Polaris»: New current internal IDS initiative
aimed to further improve the quality of IDS
Products via the major and direct involvement
of all the IDS employees in the vision of
continuous improvement.

All the steps in the logic of process improvement

Experience with non European Countries

➢ Overseas Customers (both Civil and Military) are very keen on SES Regulation independently of their application within their Country.

✓ Lack of Regulation and guidelines;
✓ They feel the need to deal also with Risks for GND ANS SW;
✓ Proactive approach toward their CAA/NSA

➢ Sometimes they require us to work as in the European Context;

➢ They demonstrate more experience with DO-178B (Dedicated benchmark required also using ED-153 Matrix)

➢ Military usually ask for higher level of SWAL (Someone asked for SWAL 1 for SW routinely assessed as SWAL 4!!);

➢ Definition of Dedicated "Certification Package" to support the acquisition of the approval to going into operation from they Regulators;

Conclusions

Perceptions:

- Clients ask for compliance with EC Reg. 552/2004 (ER.3);

- Clients ask for compliance with EC Reg. 73/2010 (Art. 8);

- Risk Assessment activities starts too late or at the very end;

- Quality/Safety Department/Functions are involved at a very late stage, sometimes with «awkward» requests;

- Not all the stakeholders are involved form the beginning;

- Misunderstanding of SW Assurance Level concept and difficulties to define SW Safety Requirements.

Conclusions

Suggestions:

➢ Elevate ED-153 as a Community Specification (EC Mandate);

➢ Involvement of the industry during the PSSA phase of a Risk Assessment process;

➢ Involvement of the Authority from an early stage of new Software implementation;

➢ Training on SW Safety for <u>all stakeholders;</u>

➢ Creation of more guidelines and/or examples on SW Safety Requirements identification and management;

➢ Never forget that SW is a component of a Functional System and safety need to be addressed at functional level.