Toward a lean approach to certification

www.open-do.org

Cyrille Comar
comar@adacore.com

Summary

Introduction to Open-DO

FLOSS & Open Source Communities

Lean/Agile vs DO-178

Why Open-DO?

Possible Open-DO material

Keys to Success

Introduction to Open–DO (1)

The Big Freeze Problem

- Can I change my code after certification ?
  - ✓ **The ESA anecdote**
- Can I upgrade to a new version of community-developed component ?
  - ✓ **The AdaCore/Gcc anecdote**

Introduction to Open–DO (2)

Which Arinc 653 OS will be around in 15 years?

Commercial Solutions

- WRS, Sysgo, LynuxWorks, GHS, DDCI

Private Solutions maintained internally by Avionics companies

- At least 3 in Europe & 1 in the US

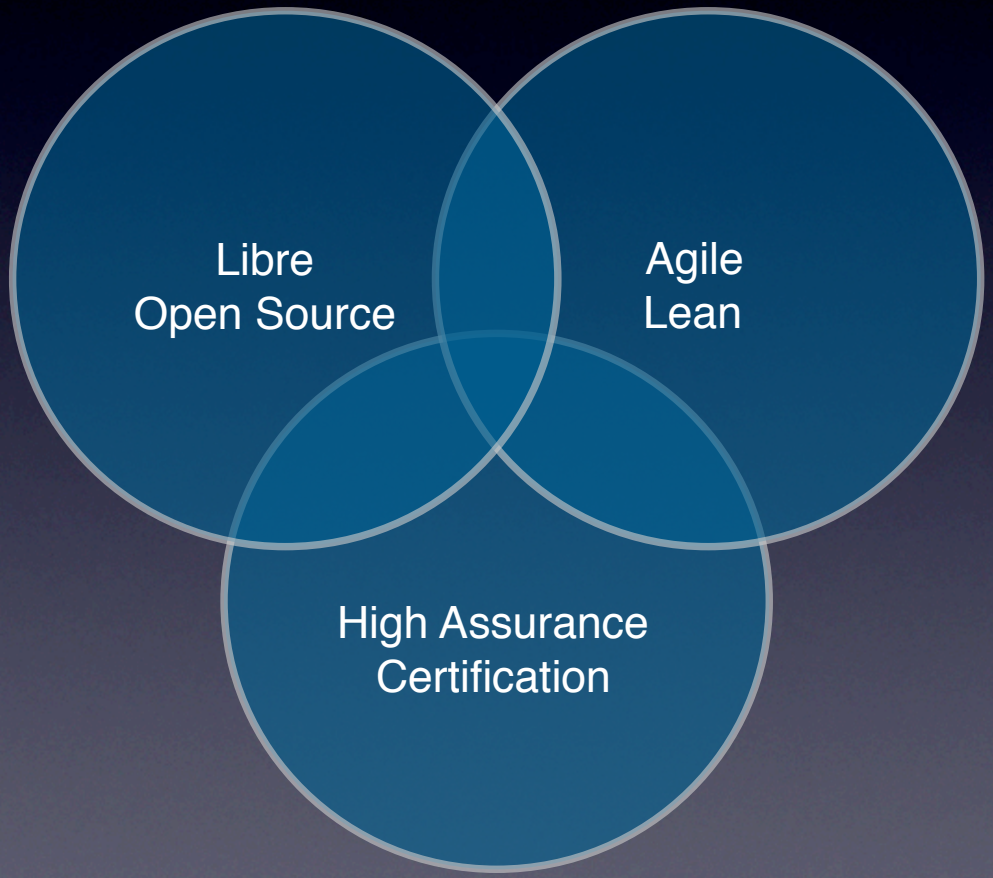
Experimental

- RTEMS + 653 interface

Any lessons from what happened in the Unix world?

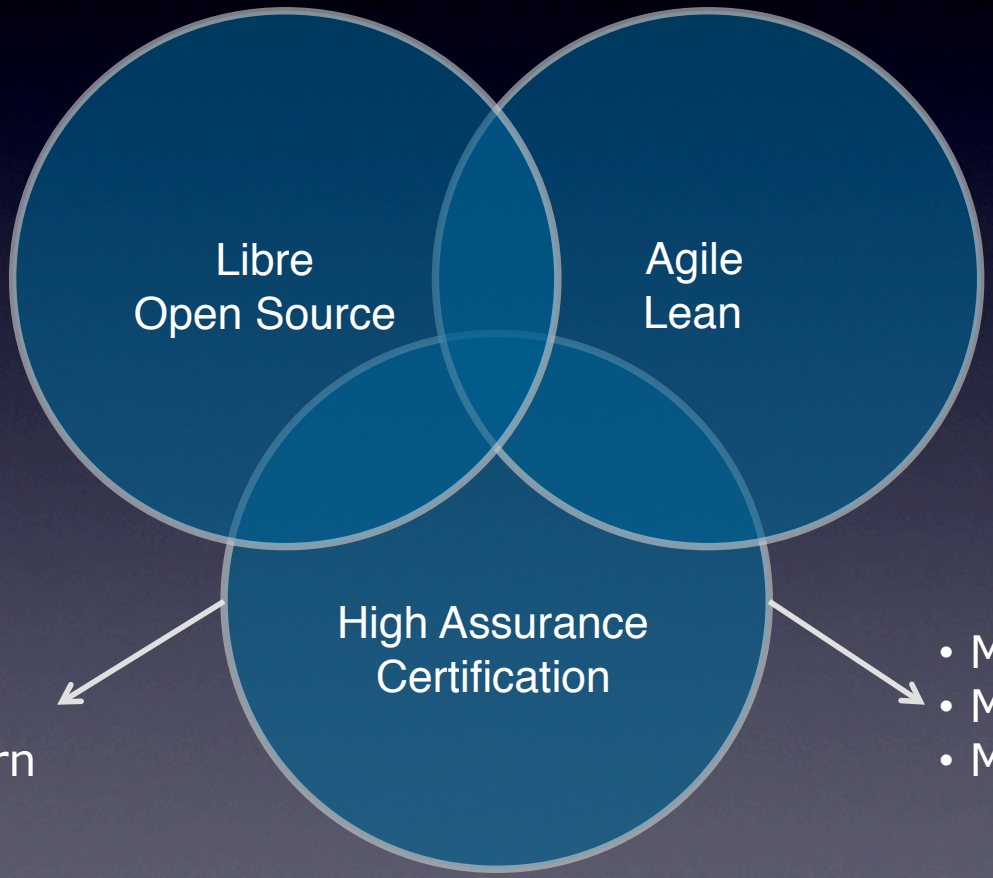
Introduction to Open–DO (3)

The meeting of 3 worlds



Introduction to Open–DO (3)

The meeting of 3 worlds

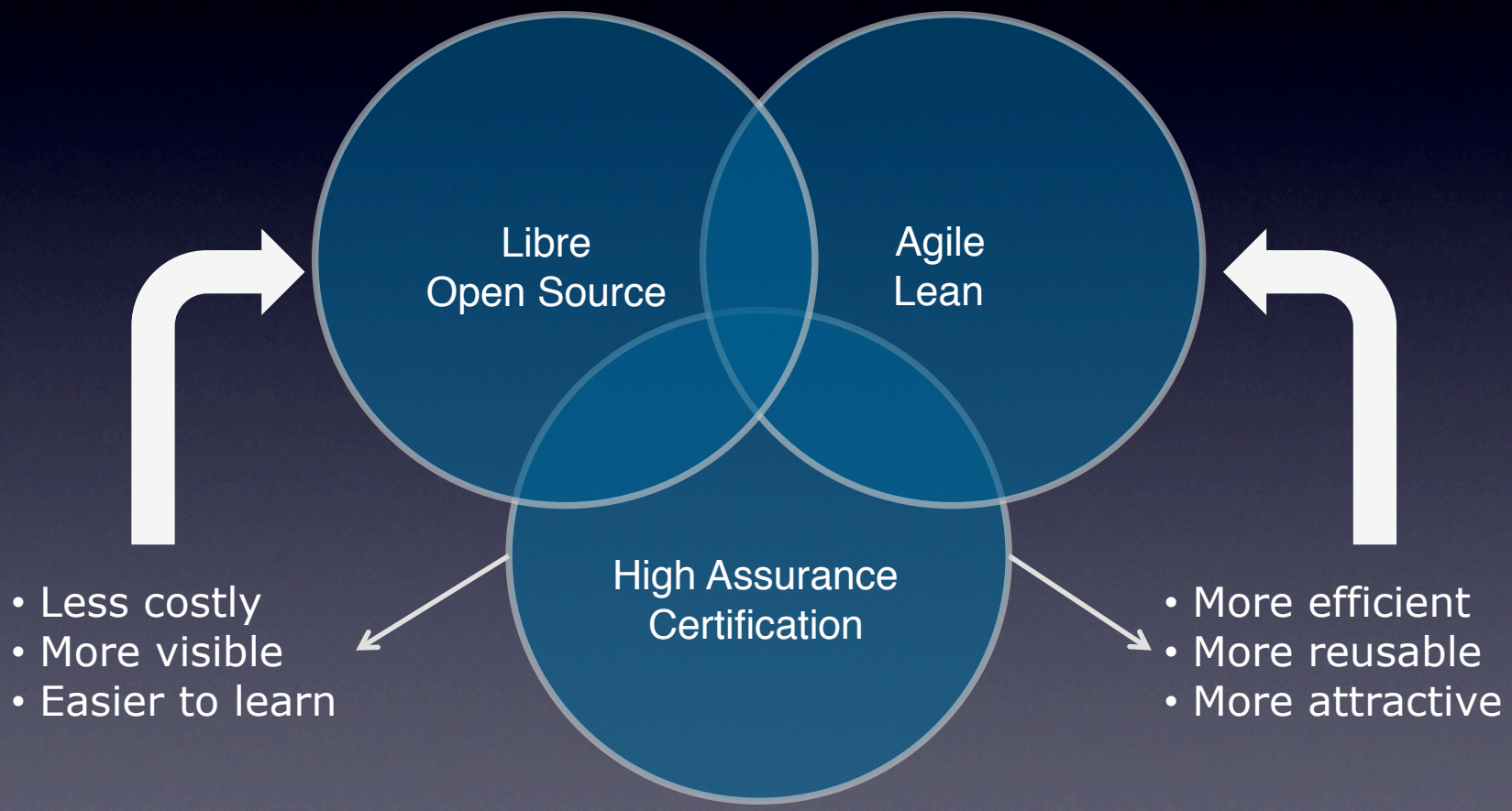


- Less costly
- More visible
- Easier to learn

- More efficient
- More reusable
- More attractive

Introduction to Open–DO (3)

The meeting of 3 worlds



- Less costly
- More visible
- Easier to learn

- More efficient
- More reusable
- More attractive

FLOSS & Open Source Communities

Open Source

FLOSS License

Free to use… for ever

Free to look at sources

Free to change

Free to redistribute

Open Source Communities (1)

Significant technologies are successfully managed by such communities:

- **The Linux Kernel**
- **Eclipse**
- **GCC**
- **RTEMS**
- **Mozilla**
- **Open Office**
- **Python**

...

For more than 20 years now

Open Source Communities (2)

- Contributors: from individuals to corporations
- Sharing technology not products

… and many more

The GCC example

Open Source Communities (3)

Active participants

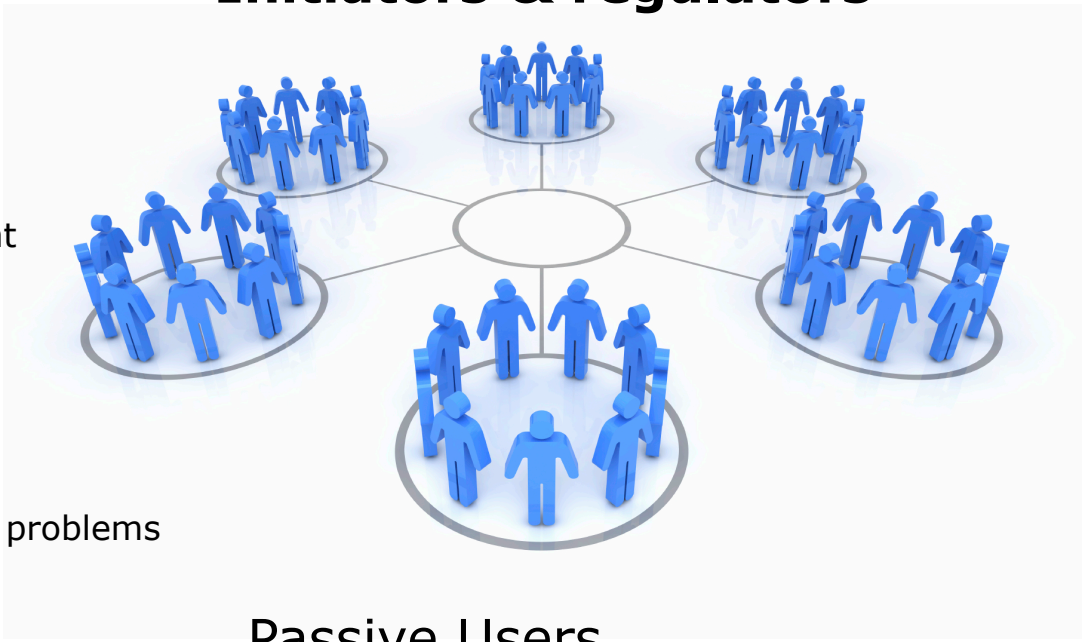
Short term cost increase

- Learning curve
- Working in an open environment
- Contributing back

Long term cost decrease by

- Sharing Resources
- Solving a common problem
- Avoiding solving already solved problems

Initiators & regulators



Passive Users

- Benefit from the work of others
- Can’t customize to their own needs
- Help spread the technology

Open Source Communities (4)

Sharing instead of Off-shoring

COTS or not COTS?

- **What about the HA/certification community?**
- **Is there a need for openness & cooperation?**
- **Potential for community growth?**

- military
- space
- railways, automotive, …

- AVSI (Aerospace Vehicle Systems Institute)
- Certify Together
- The DO-178C committee

Lean/Agile vs DO-178

DO-178 vs Lean/Agile

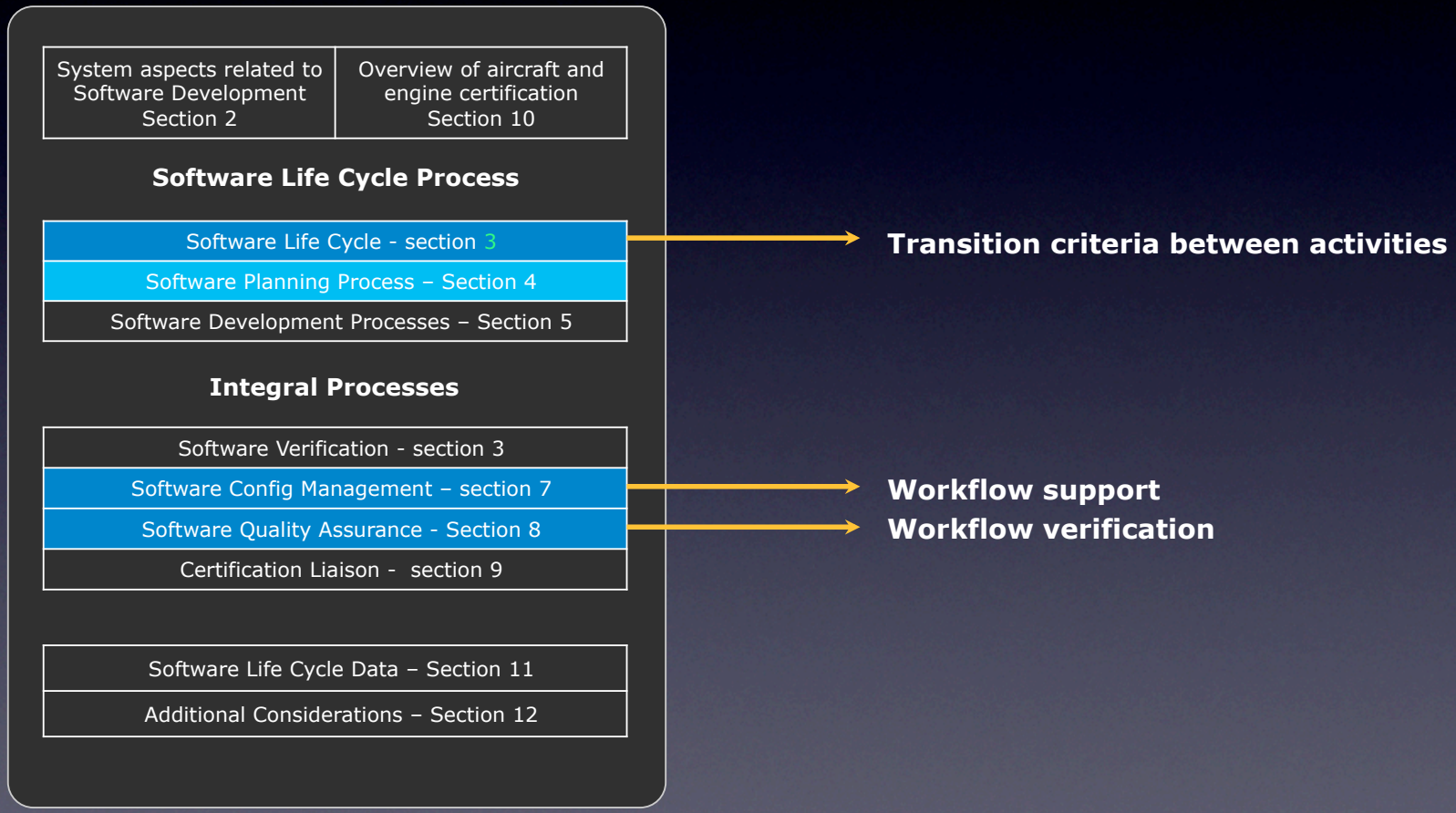
- Life Cycle Data & Traceability
- Specific Workflows
- Requirement Based Testing
- Emphasis on verification activities

- Continuous Integration
- Iterative requirements
- Test Driven Development (Executable Specifications)

- Good Software Engineering Practices
- Guarantee/Improve Quality

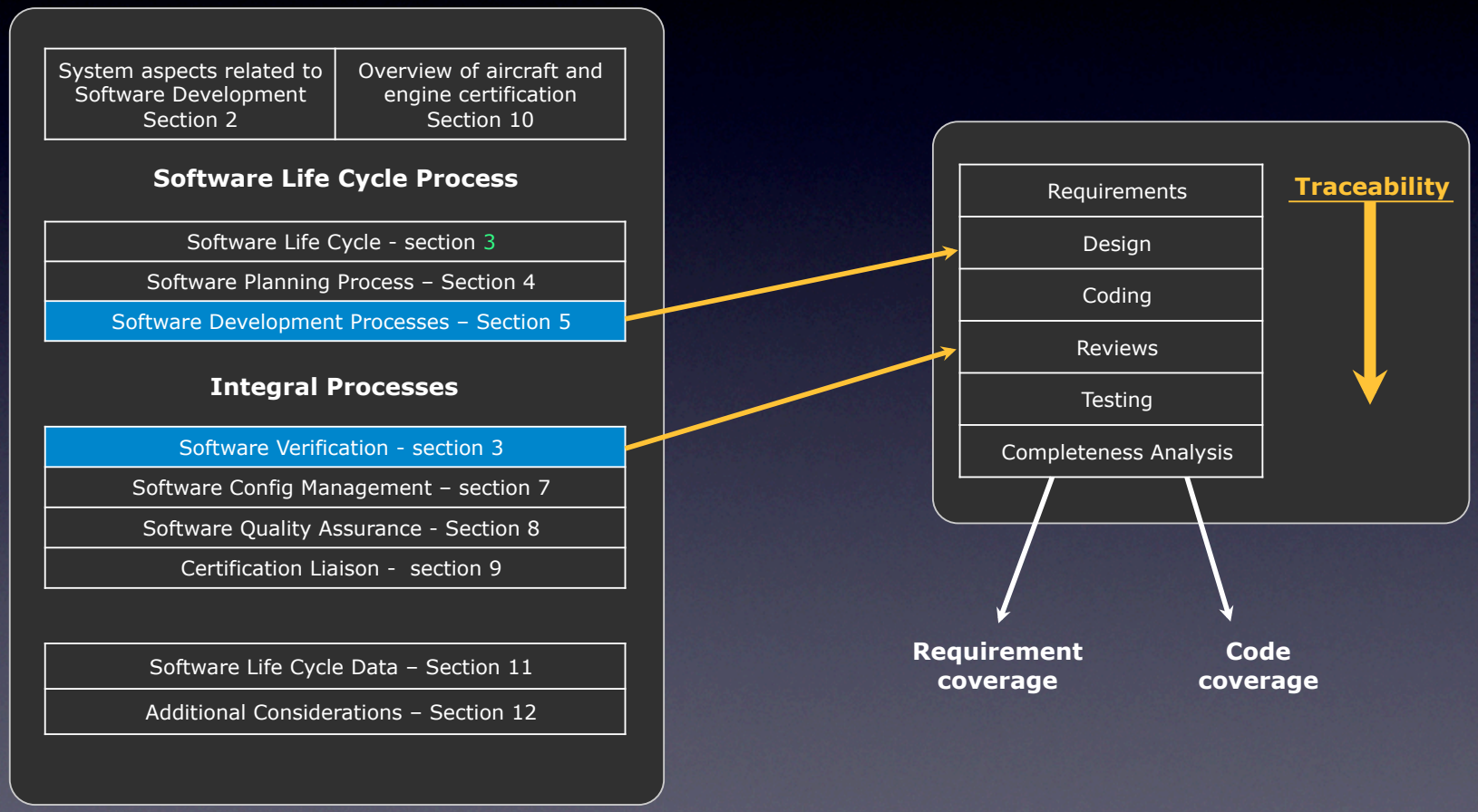
Some DO-178B workflows (1)

Top level workflow



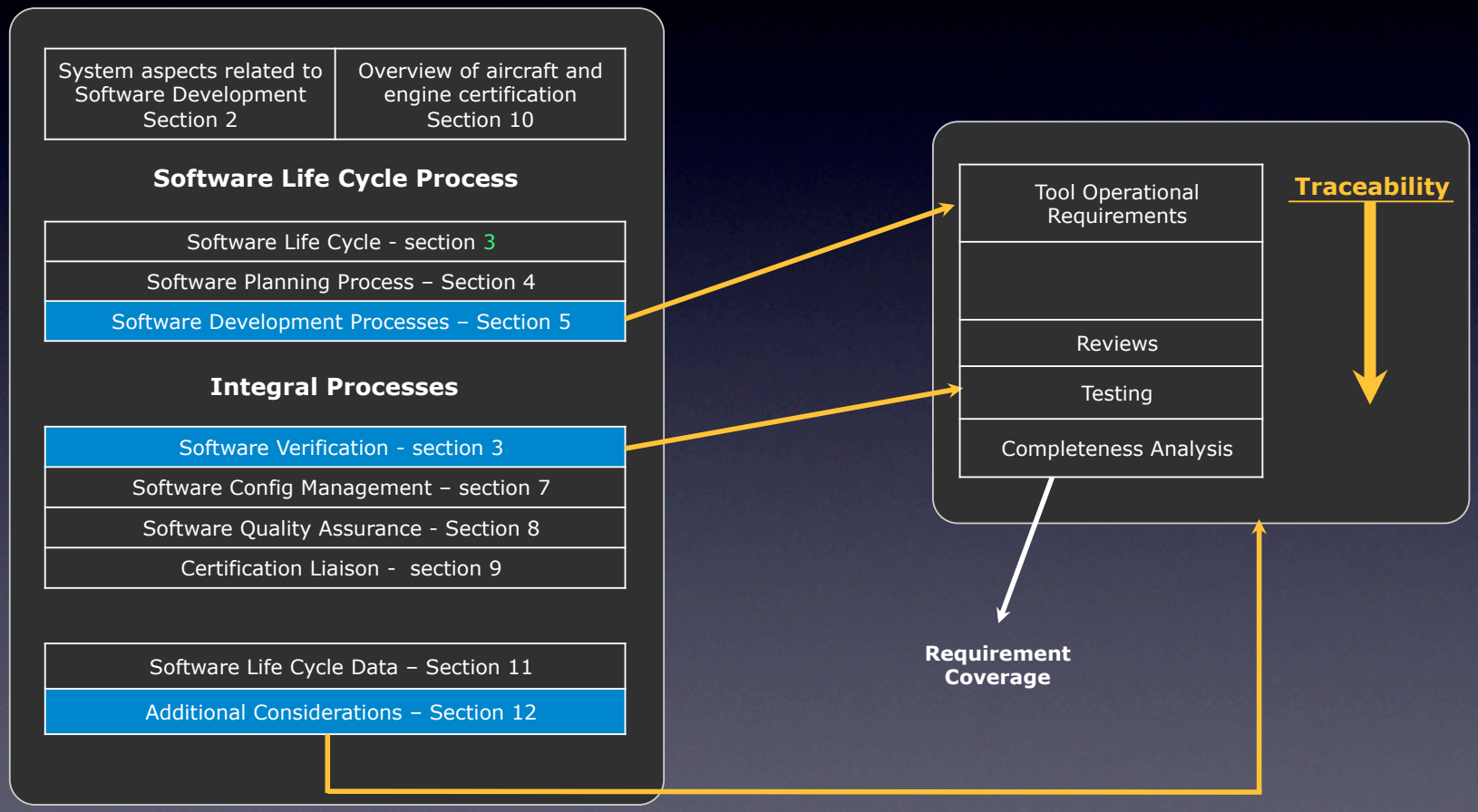
Some DO-178B workflows (2)

Component certification workflow



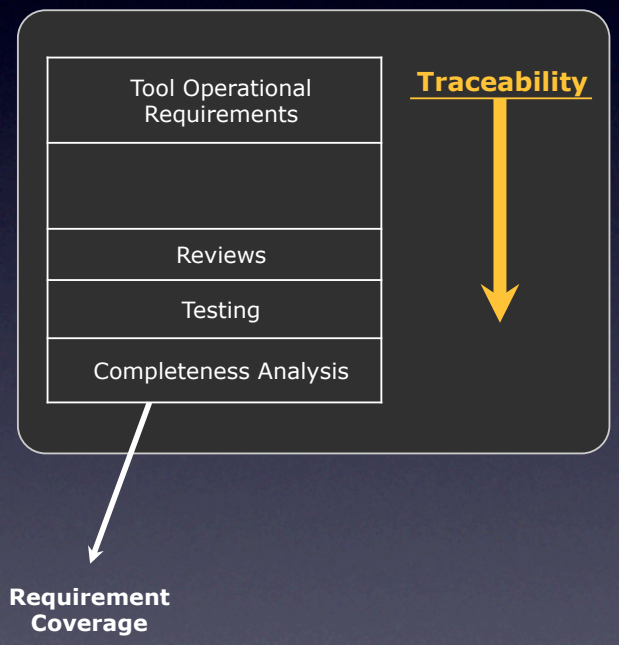
Some DO-178B workflows (3)

Qualification of Verification Tools Workflow



Example : Agile Tool Qualification

- Minimize requalification effort when adding a new TOR
- Automate requalification for different environment
- « Natural » traceability model
- Integrate QA & CM

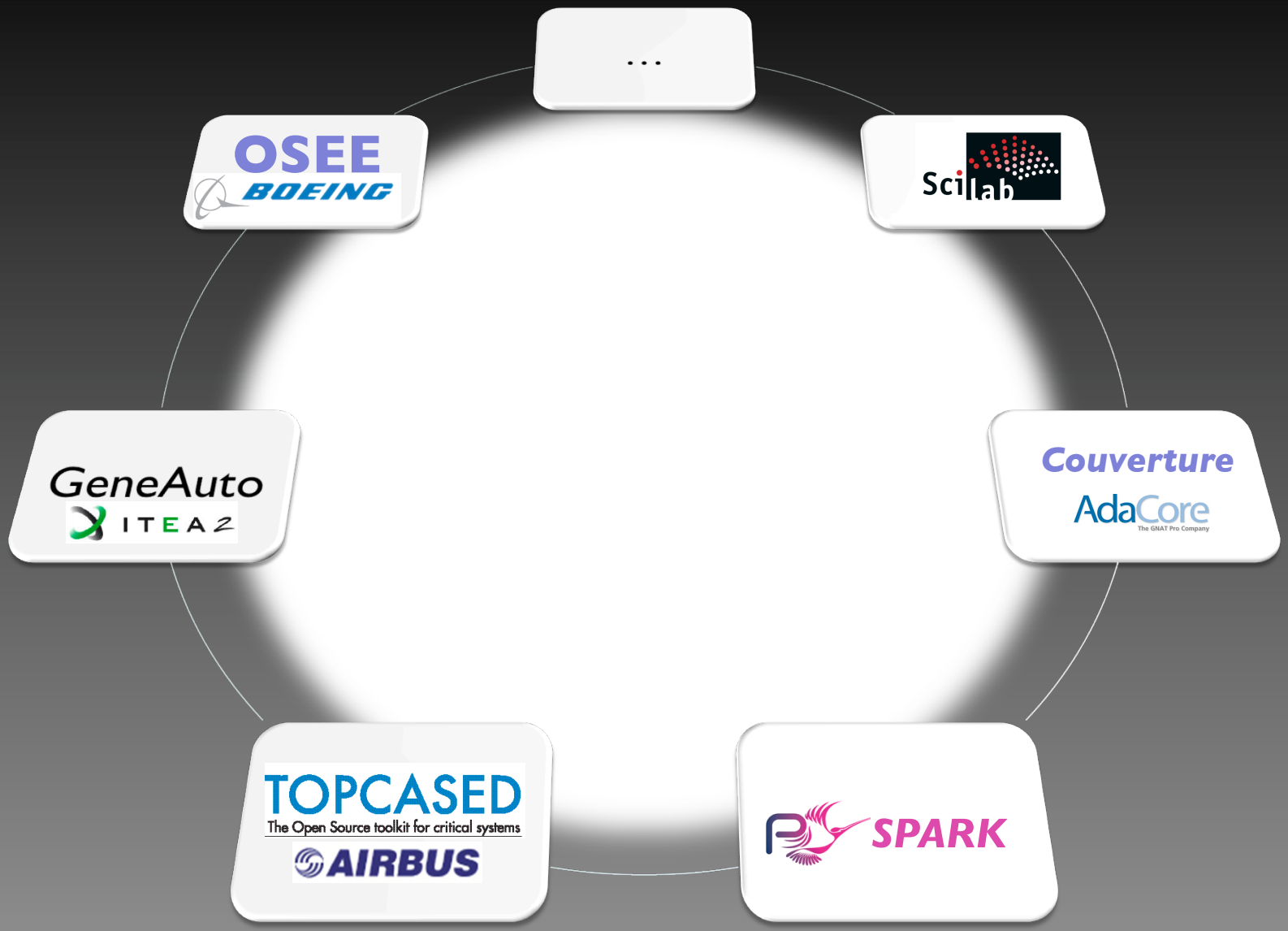


2 running experiments

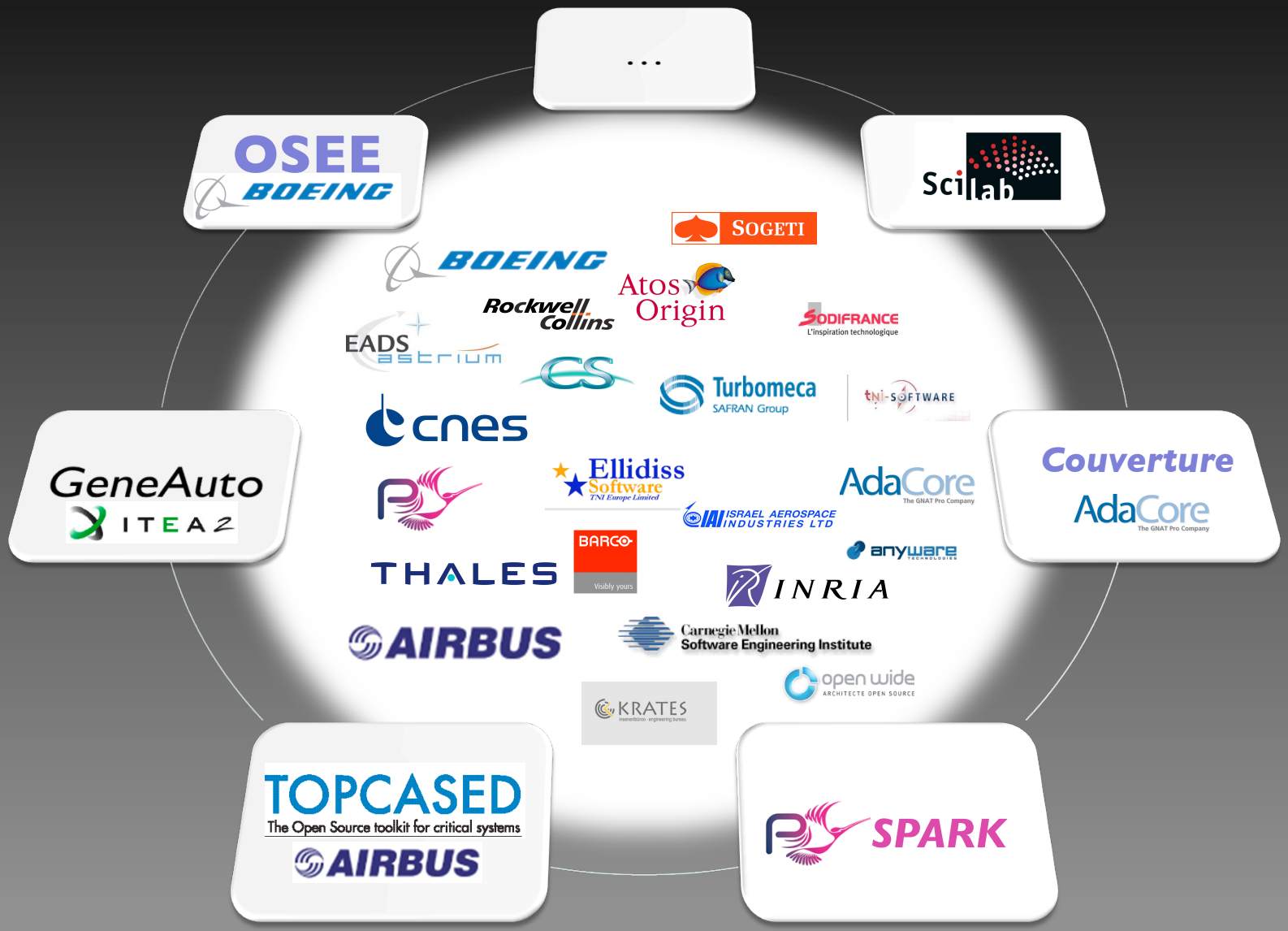
OSEE **FitNesse +SVN**

Possible Open-DO material

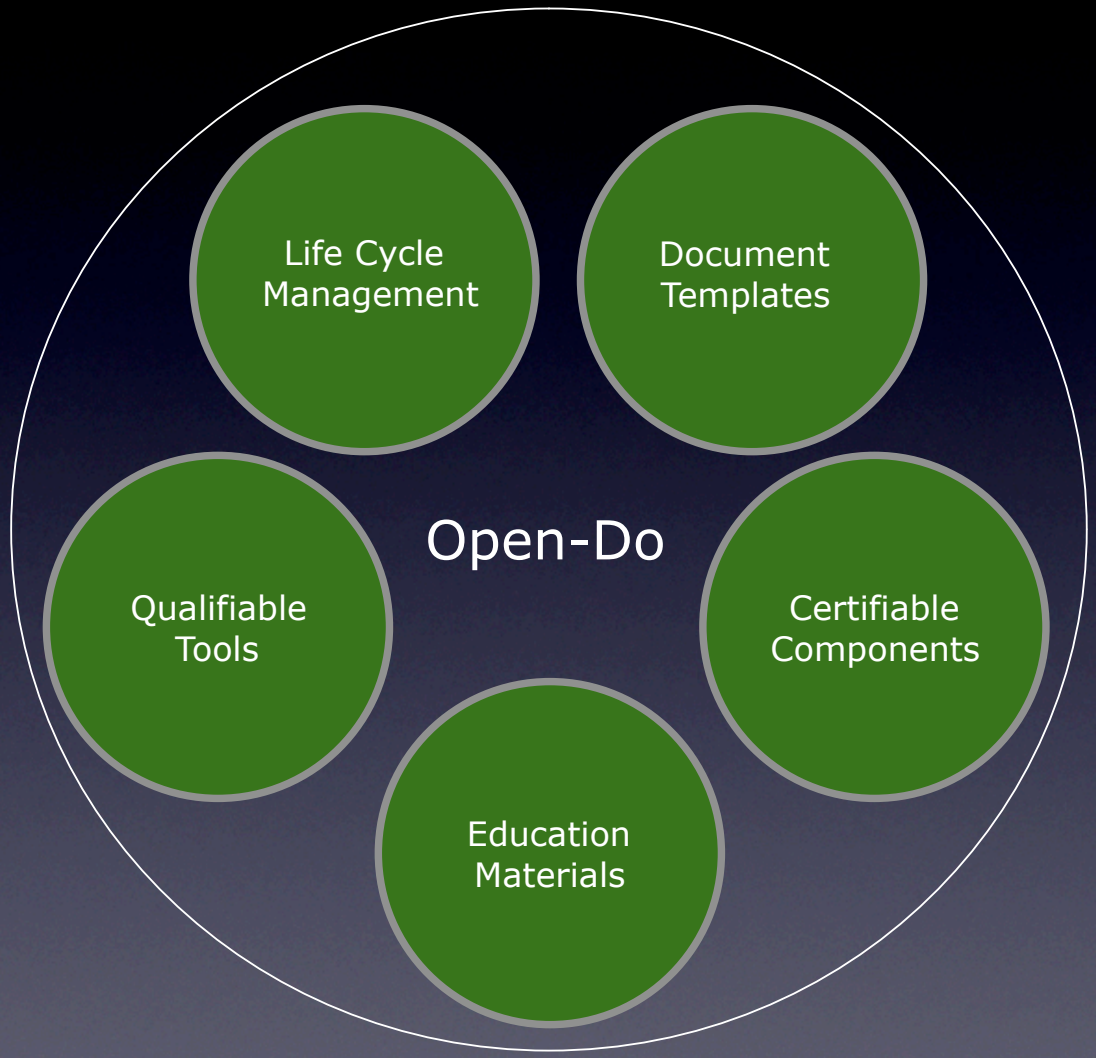
Some Relevant Open Projects & Technologies



Some Relevant Open Projects & Technologies

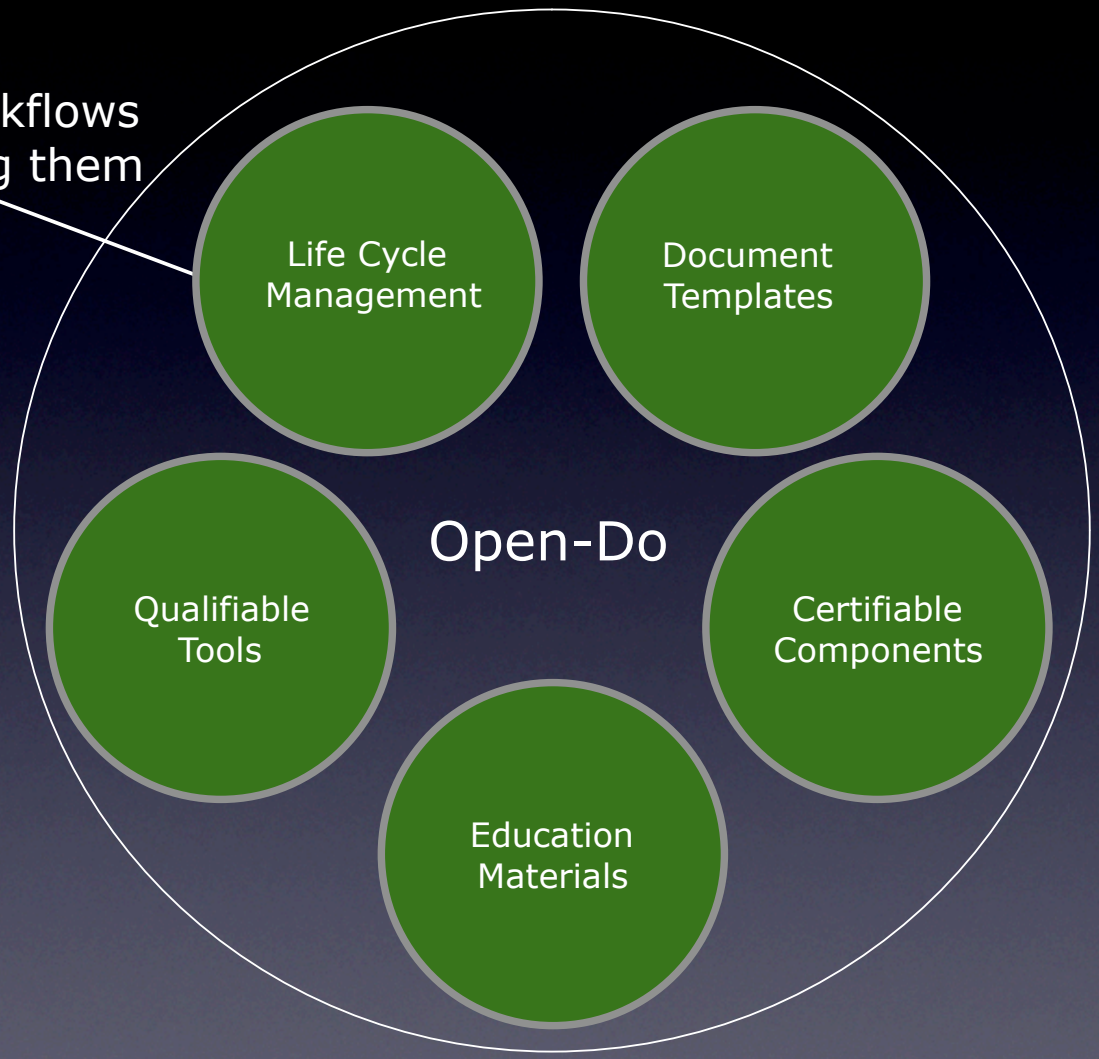


Open DO Components

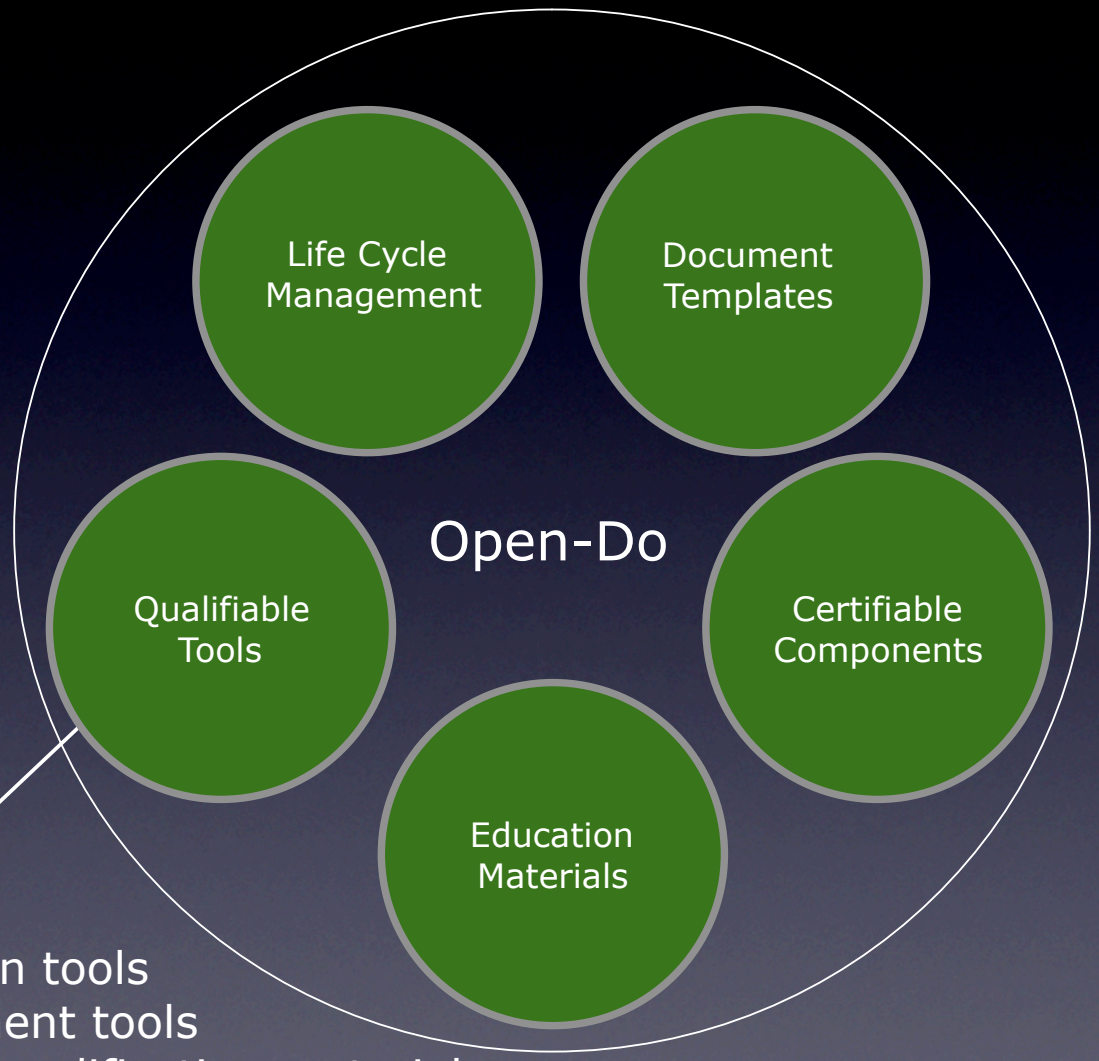


Open DO Components

- Specialized Workflows
- Tools supporting them

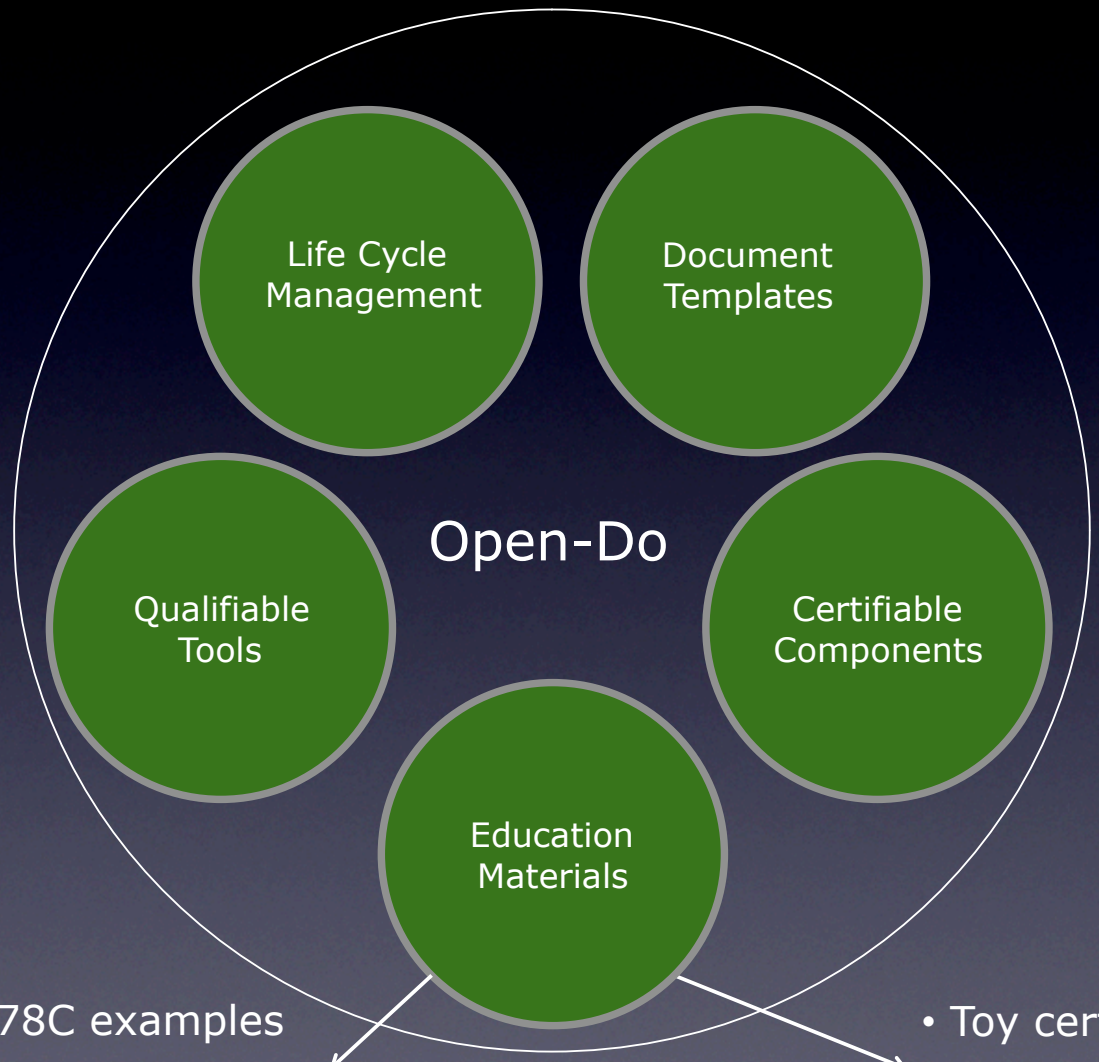


Open DO Components



- Open verification tools
- Open Development tools
- Open (orphan) qualification material

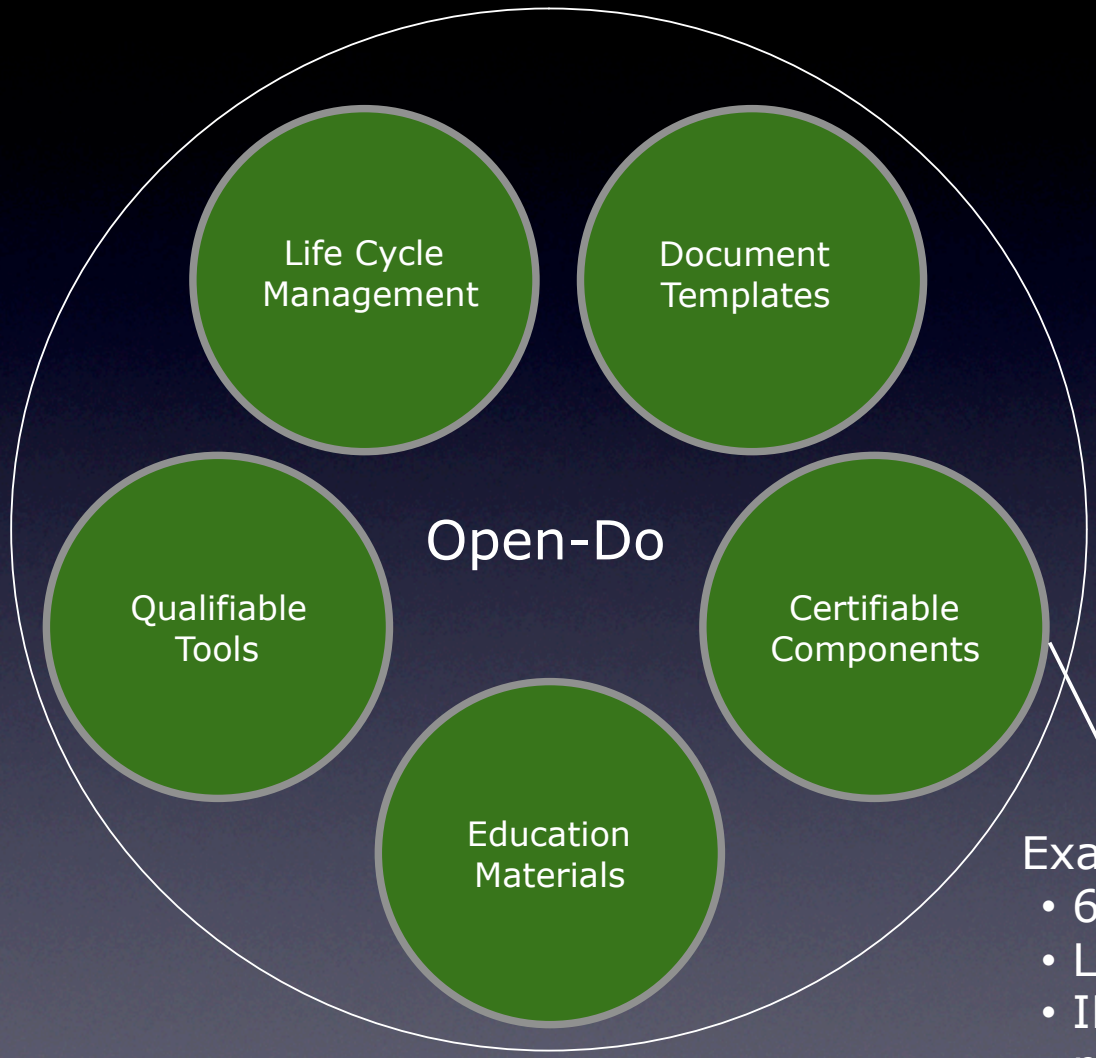
Open DO Components



- Specialized DO-178C examples
  - Model Based
  - Formal Methods
  - OOP …

- Toy certifiable projects
- Training material

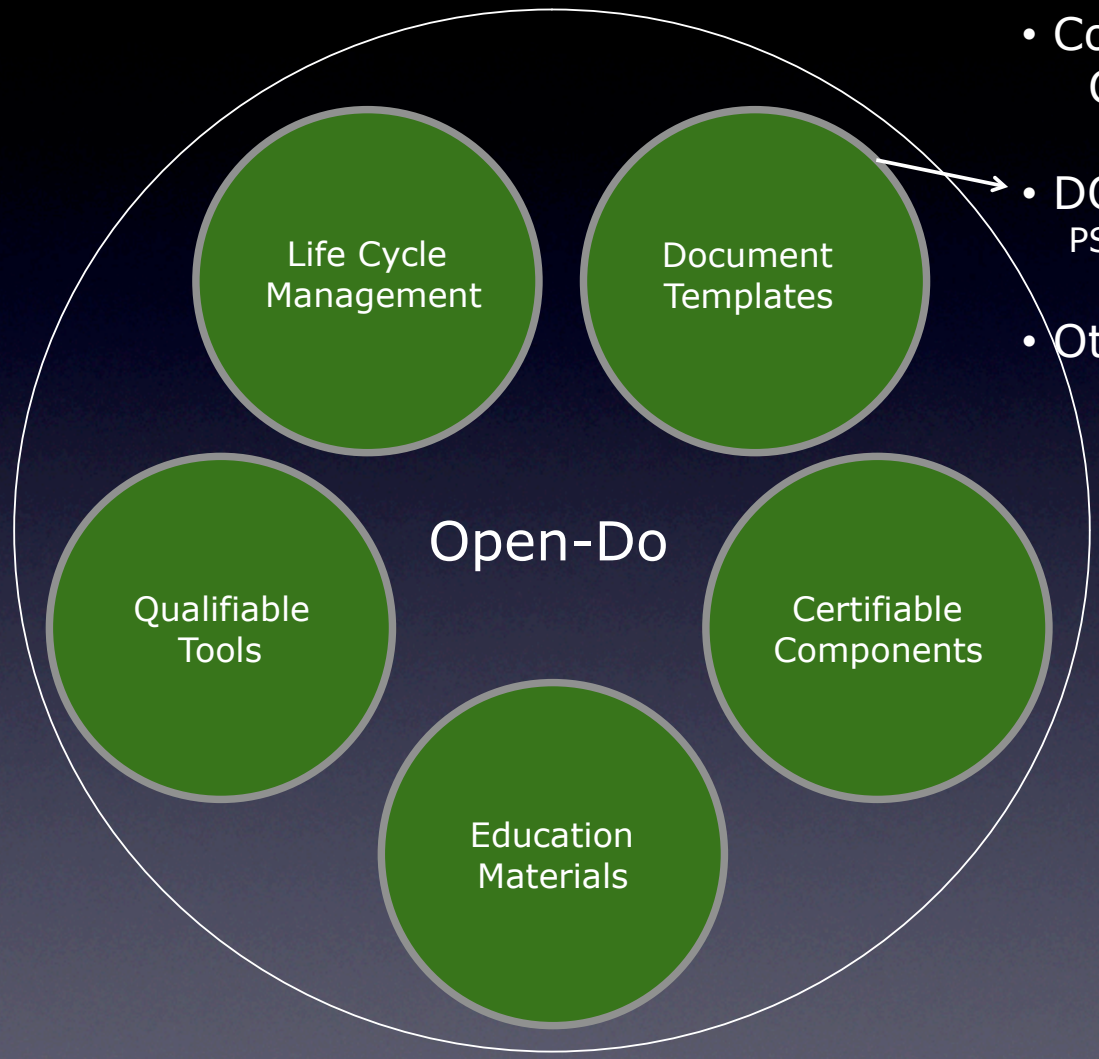
Open DO Components



Examples:

- 653 OS
- Light DataBase
- IP stack
- middleware
- Standard Classes
- …

Open DO Components



- Coding Standards
  C, Ada, …
- DO-178:
  PSAC, SDP, SVP, SCMP…
- Other standards

Why Open-DO ?

Why Open-DO?

Avionics industrial community

Provides a shared infrastructure

- For long term investment
- For long term cost reduction

Allows some level of cooperation with competitors

Lower training costs (especially for subcontractors)

Support for the transition to DO-178C

Why Open-DO?

Academics

Better understand the needs of this industry

Offer adequate training to students

Opportunity for applied research activities

Why Open-DO?

Tool providers

Offers an ideal showcase for their open technologies

Tool sharing makes it easier to provide a complete supported solution

Creates and ecosystem where everyone can meet potential customers and partners

Keys to success

Balance

- Europe vs US
- Boeing vs Airbus
- Authorities vs Industry

Find key participants for critical mass

- Certification authorities
- Major Aeronautics players
- Established tool providers
- Academics

Attract public funds for bootstrap

Find appropriate governance rules

Open-DO Bootstrap

- One project in Europe (FP7)
  - call for projects in 1 month (T0)
  - submission of the proposal : T0 + 4 months
- One project in the US
- Others?

Share from the start
- infrastructures
- ideas
- activities

open-do.org