AdaCore
The GNAT Pro Company

Efficient Safety Critical Systems Development

Is FLOSS the only answer?

Michaël Friess
Sales & Business Development Manager

Cyrille Comar
Managing Director

Class 12 - FLOSS for Safety Related Systems

Embedded World Conference 2011

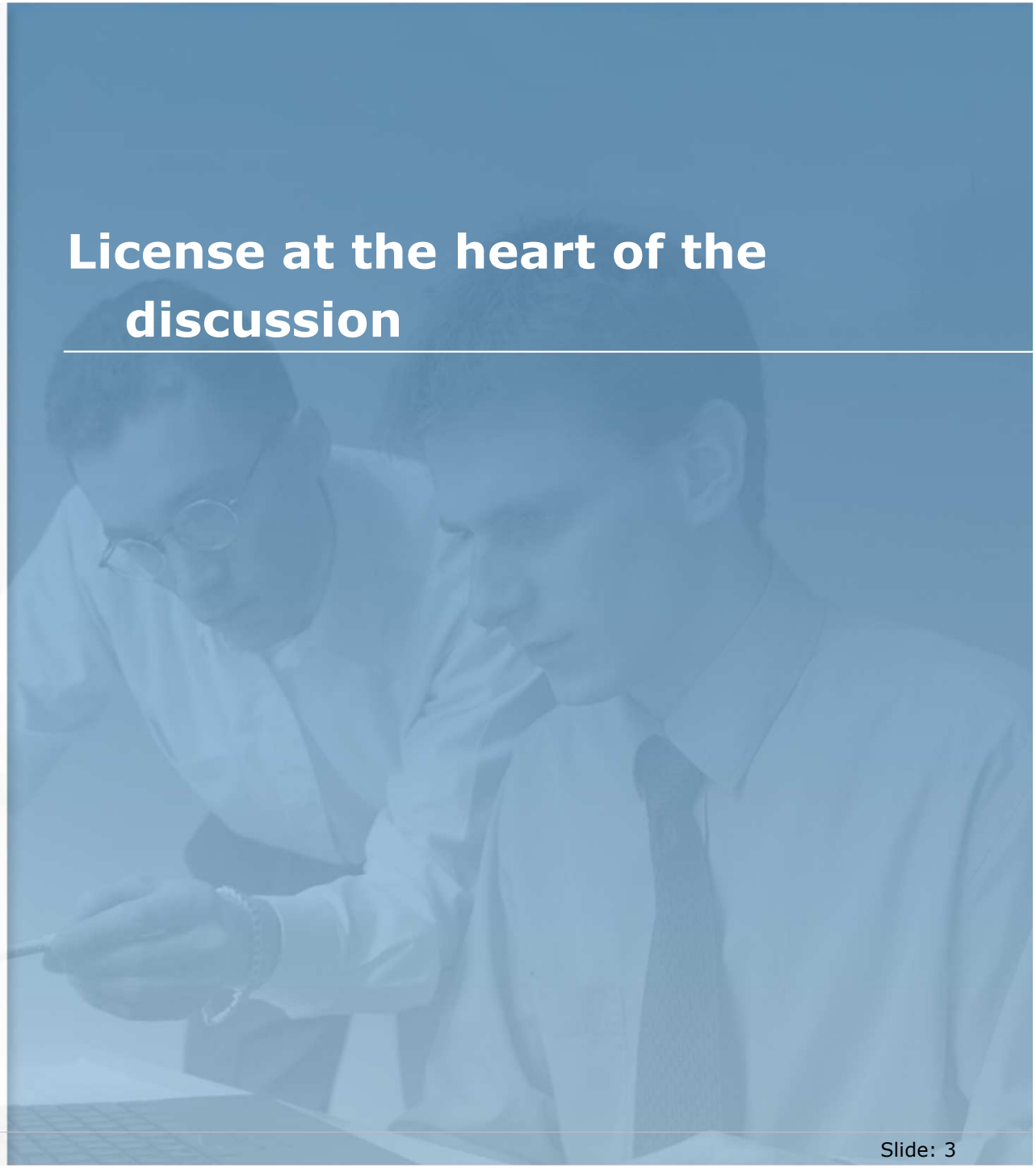
Let's imagine...

- A cooperative and open framework for the development of certifiable software
- Competitors who work together to share costs
- Software that is easy to certify and to recertify

Weird idea, isn't it?

AdaCore
The GNAT Pro Company

License at the heart of the discussion



FLOSS is just about software license

- **FLOSS = Free/Libre/Open Source Software**
- **Free/Libre/Open Source:**

  properties of a license provided by the copyright owner

FLOSS License

- **Free to run**
- **Free to look at the sources**
- **Free to change**
- **Free to redistribute**

FLOSS and Restrictive Licenses – The Common Base

- The software is copyrighted
- It cannot be copied or used without a license
- The license allows certain rights to copy and use the software

FLOSS and Restrictive Licenses – The Differences

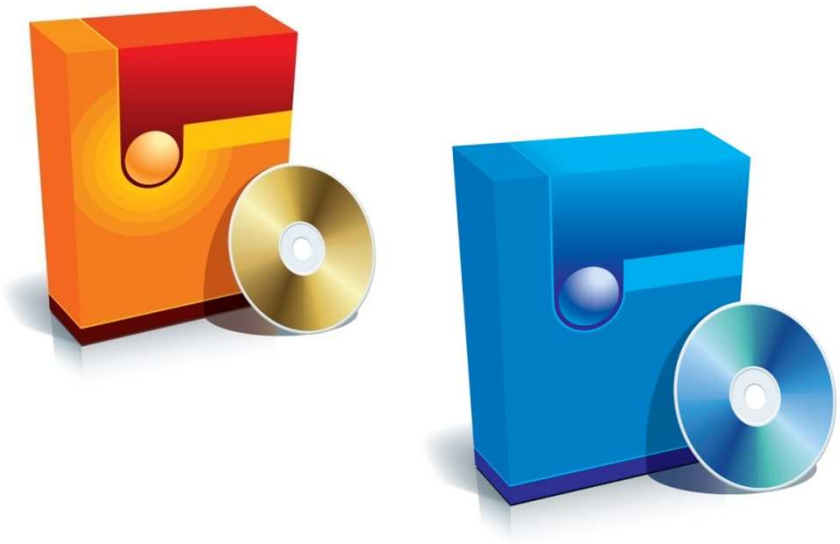
- **In the license terms:**
  - License conditions are very different
  - Restrictive License: strictly limits usage and copying
  - FLOSS License: far more liberal, less restrictions (usage and copying rights are a superset of Restrictive Licenses)

Topics to consider for both FLOSS & Restrictive Licenses

- Provenance (trust)
- Support
- Product evolution
- Maintenance
- The price to pay for the combination of: software, support, and license

Is FLOSS appropriate for safety related systems?

- At worst, license is neutral
- Most probably, a FLOSS License provides an advantage over a Restrictive License



AdaCore
The GNAT Pro Company

COTS vs. Bespoke

COTS – Commercial Off-The-Shelf – Product

The market answer for sharing costs for the

Creation

Industrialization

Support

Maintenance

Repair

Evolution

of software amongst users having similar needs

The License of a COTS

Restrictive License

FLOSS License

A High Demanding Customer Base

LOCKHEED MARTIN

MDA

NATS

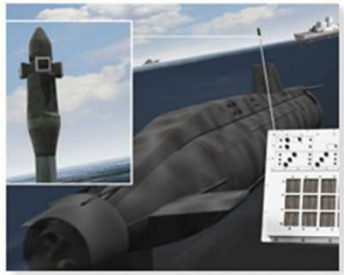
Raytheon
Integrated Defense Systems

AnsaldoSTS

Martin-Baker

THALES

THALES



Atos Origin™

BOEING

EADS Astrium

EADS CASA

BAE SYSTEMS

The Job of a FLOSS Vendor

- **COTS is often made of SW from many SW communities**
  - Need for integration
  - Need for version management
  - Need for QA

- **Ability to interact & participate to these communities**
  - To maintain the SW
  - To make the SW evolve
  - To integrate new features

- **Understand licensing**

FLOSS Gives You Many Options

Getting the FLOSS

- Buy the FLOSS from a vendor

  => COTS

- Download the FLOSS as-is

  => Bespoke

Getting help

- Do nothing
- Build in-house expertise
- Become part of the development community
- Purchase Services

Your Choices with FLOSS

- Download the FLOSS and use it
- Build in-house expertise
- Become part of the development community
- Purchase COTS

COST vs. RISK analysis

AdaCore
The GNAT Pro Company

Safety Related Software is NOT just Software

What is Safety-Critical Software?

Context:

- **Safety-related piece of software**
- **Definition of a Safety-Integrity Level**
- **Certification standard, like:**
  - Avionic: DO-178B
  - Railway transportation: IEC 61508
  - Automotive: ISO 26262 (forthcoming)

Corollary:

- **Establishment of a development process (requirements, test, verification, etc.)**
- **Documentation artifacts aka. Software Certification Artifacts**

What Safety-Critical Software Looks Like

Software Code

- **Object code/Executable**
- **Source code**

Certification Evidence

- **PSAC** (plan for software aspects of certification)
- **SDP** (SW development plan)
- **SVP** (SW verification plan)
- **…**

Reverse-Engineering of Existing SW into Safety-Critical SW

A risky operation

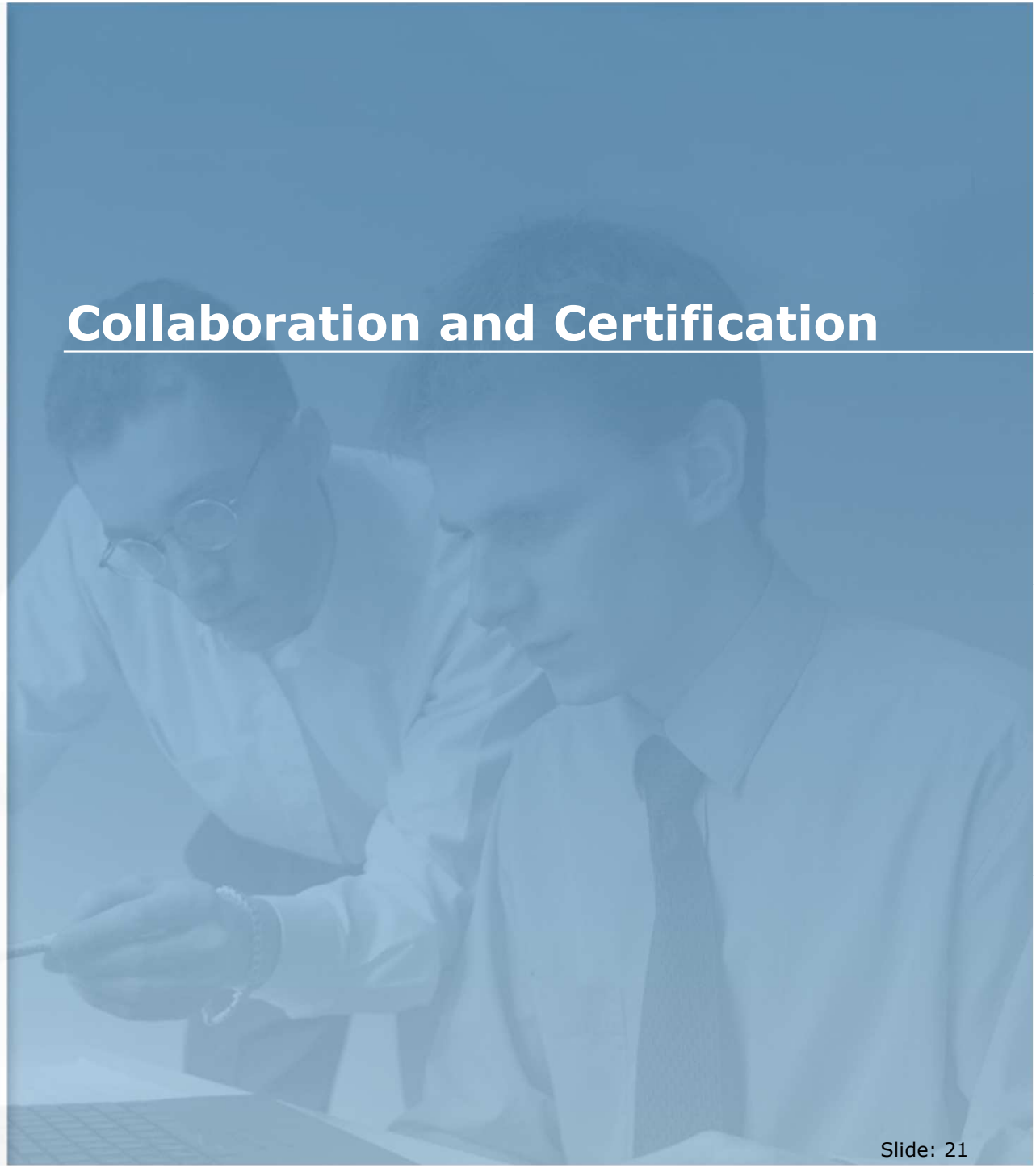
- Safety properties often carried by SW architecture and design
- Stringent requirements adapted to the SIL
- The result of a well-defined development process

FLOSS and Safety Related Systems

- **FLOSS**
  - The freedom to choose the best approach (Bespoke vs. COTS)
  - As a COTS: additional safeguards compared to restricted licensed SW
  - In the context of safety related systems:
    - Access to source code eases the handling of certification evidence
- **Safety Related Systems**
  - Source code: only part of the equation
  - How to handle certification evidence?

AdaCore
The GNAT Pro Company

Collaboration and Certification



The Open-DO Initiative

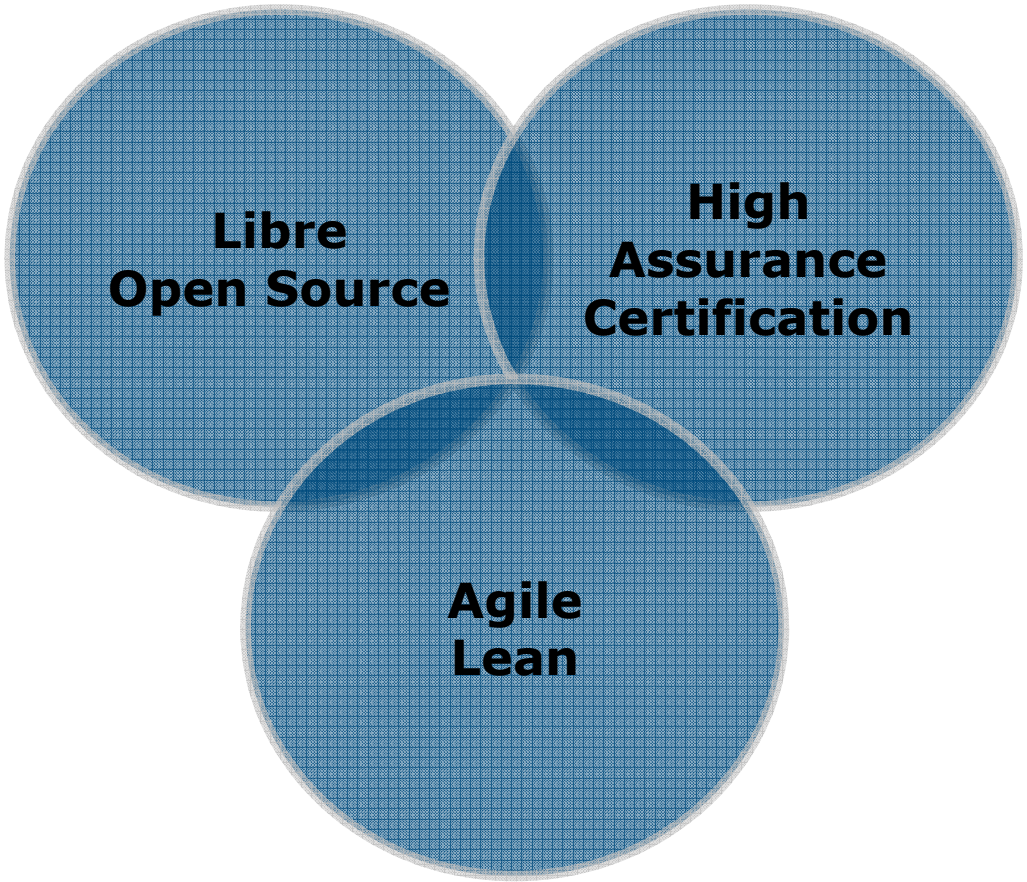
openDO

- Towards Cooperative & Open Framework for the development of certifiable SW
- FLOSS model to share costs
- FLOSS that encompasses certification artifacts
- Agile methods at the heart of its development process

⇒ Towards continuous certification

http://www.open-do.org

Open-DO – At the Crossroad of 3 Worlds



AdaCore
The GNAT Pro Company

Highlight on the Qualifying Machine

Why Qualifying/Certifying?

- **Tool qualification**
  - Substitute manual activities with a tool
  - No need to verify the output of the tool
  - Ex: checking for a coding standard, coverage analysis, model-based code generation, …
- **COTS certification**
  - Reuse a certification kit across different projects
  - Ex: Ada run-time library, XML library, …
- **Problem: The Big Freeze**
  - Qualification/Certification = Baselining
  - How can you evolve a technology which requires qualification?

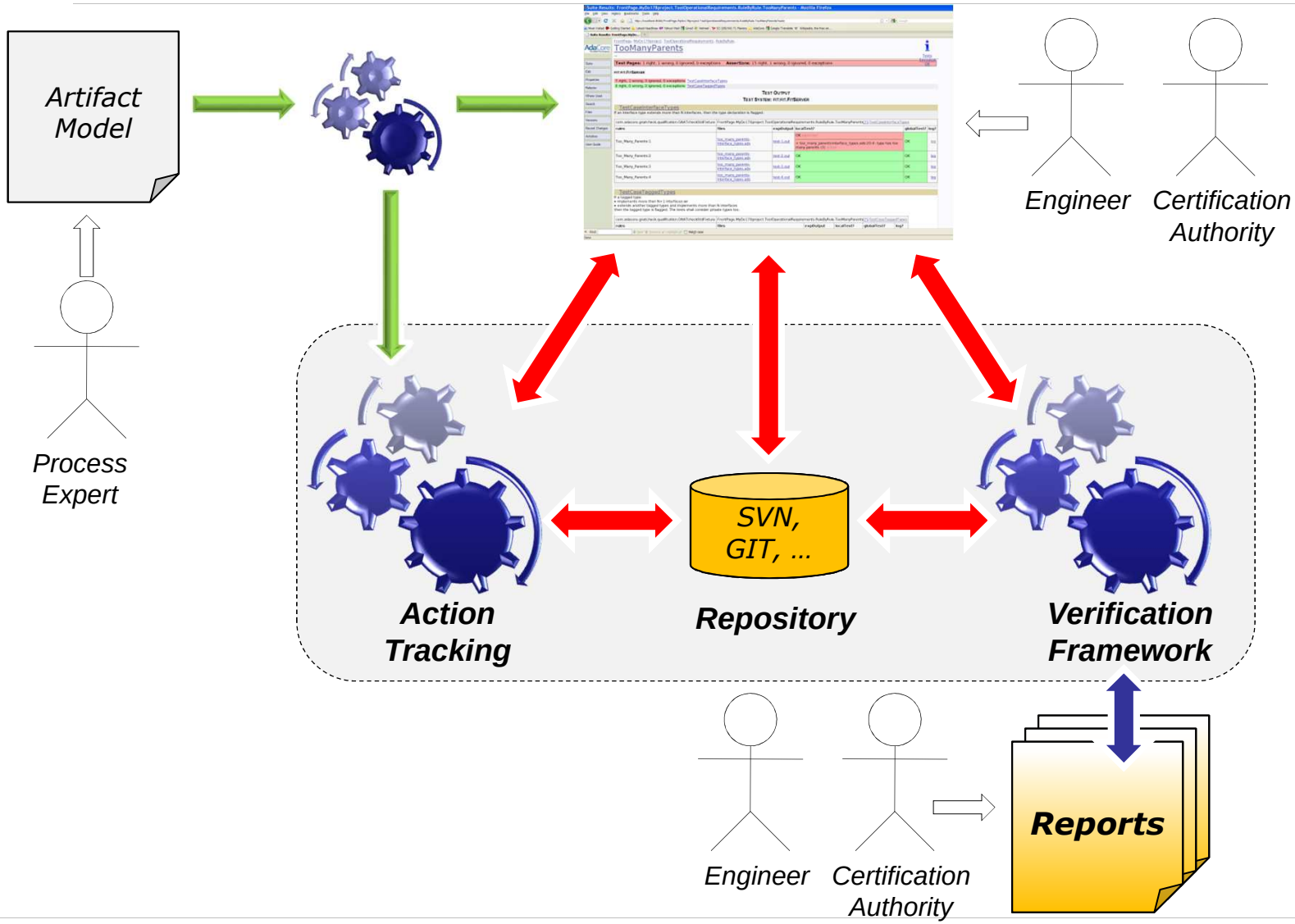
Qualification Machine: the goals

- **Delta qualification**
  - A new requirement arises on an already qualified tool
  - What is the minimum effort to re-achieve qualification?

- **Continuous qualification**
  - A tool shall always be in a "semi-qualifiable" status
  - Mirror the "continuous integration" concept
  - At any time, you should know:
    - Which artifacts shall be produced to achieve qualifiability
    - Which activities shall be performed to achieve qualifiability

- **Automation**
  - Automatic production of (part-of) qualification evidence
  - Focus on traceability, coverage and workflow management/tracking

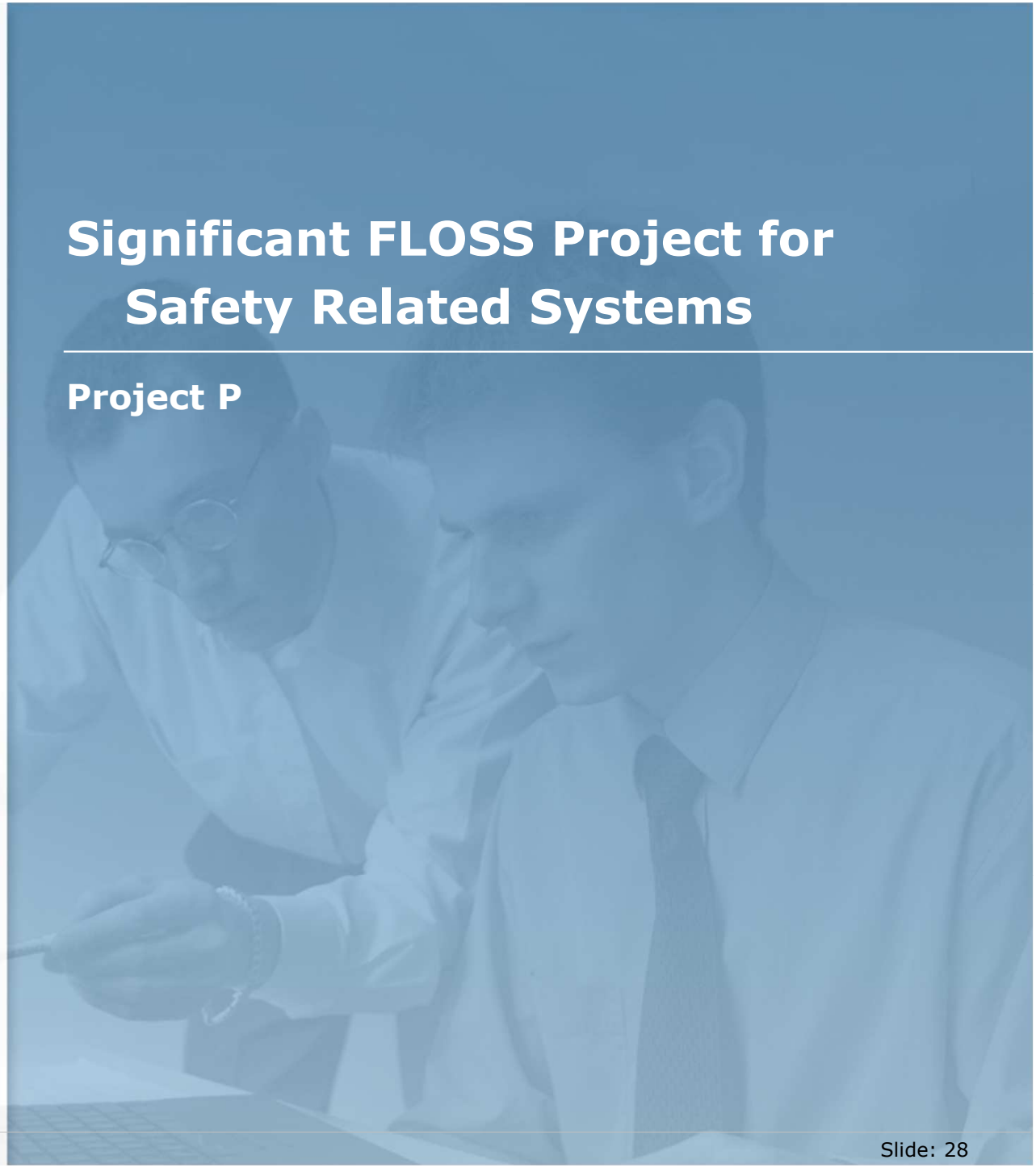
The Qualifying Machine



AdaCore
The GNAT Pro Company

Significant FLOSS Project for Safety Related Systems

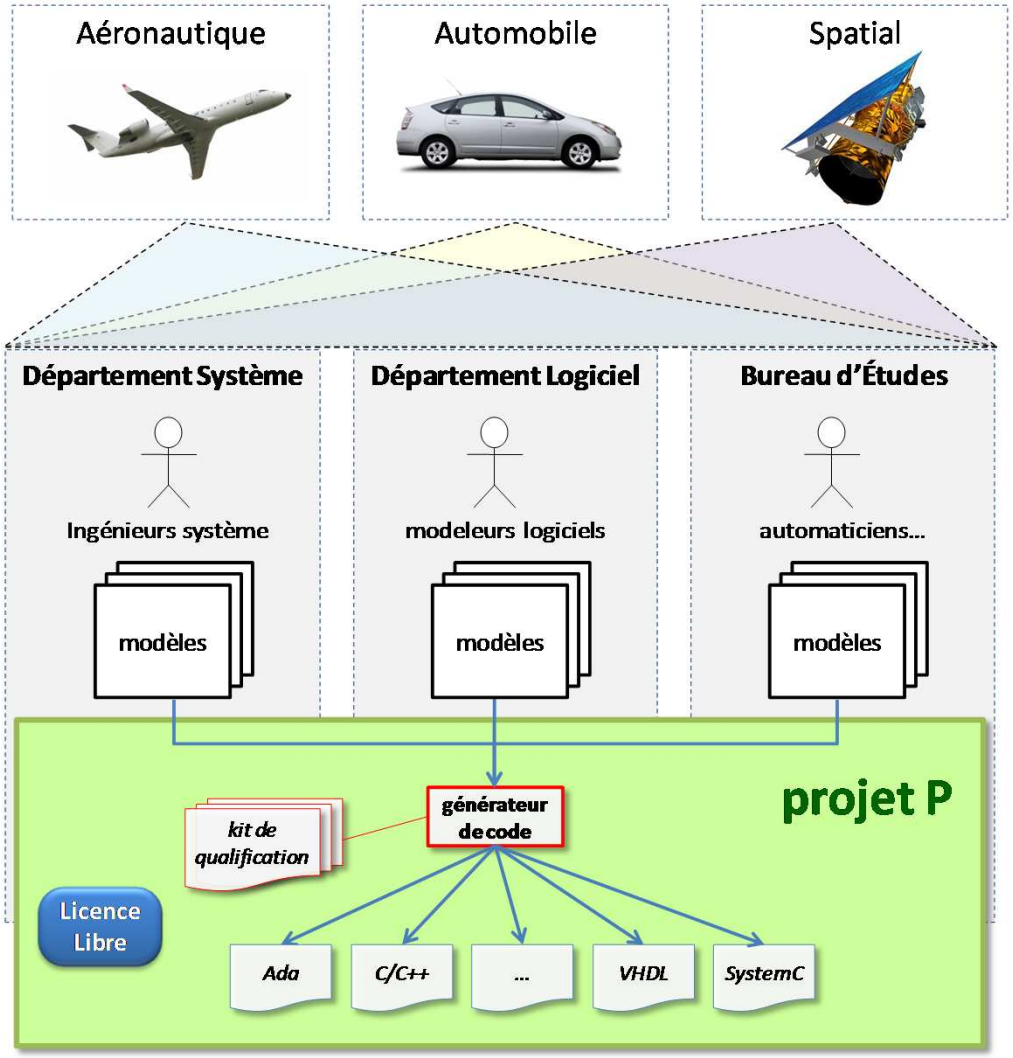
Project P



Project P in a Nutshell

- Cooperative development supported by the French government (official announcement: March 1st, 2011)
- FLOSS license
- Eases the development of real-time safety-critical systems
- Leverages on model oriented engineering seconded by automatic code generator
- Development of a qualification kit for the code generator

Project P in a Nutshell



Project P - FLOSS for Safety Related Systems

- **Duration: 36 months**
- **Investment: nearly 10 million euros**
- **19 partners, including:**
  - AdaCore
  - Airbus
  - Astrium
  - Atos Origin
  - Continental
  - Rockwell Collins France
  - SAGEM Defense
  - Thales Alenia Space
  - Thales Avionics
  - …

AdaCore
The GNAT Pro Company

Thank you for your attention

michael.friess@adacore.com
Hall 11, F224