Towards a Lean Tool Qualification Process

Digital Avionics Systems Conference

Tucker Taft, AdaCore, taft@adacore.com
Matteo Bordin, AdaCore, bordin@adacore.com

AdaCore

Our personal feelings towards tool qualification

All Kinds of Torture

GNATcheck, DO-178B Ver. Tool,
Airbus Military, A400M, 2010

GNAT Pro Compiler, EN-50128 T3,
CERTIFER, 2014

CodePeer DO-178B Ver. Tool,
Utas UK, A400M, 2014

Runtime, DO-178B level A
GE, 787, 2009

GNATcoverage DO-178B Ver. Tool,
Thales Avionics, A350xwb, 2010

http://en.wikipedia.org/wiki/Torture

Runtime, EN-50128 SIL 3/4
CERTIFER, 2014

Runtime, ECSS-E-40 level A
Astrium ST, Sentinel, 2010

GNATtest, EN-50-128 T2,
CERTIFIER, 2014

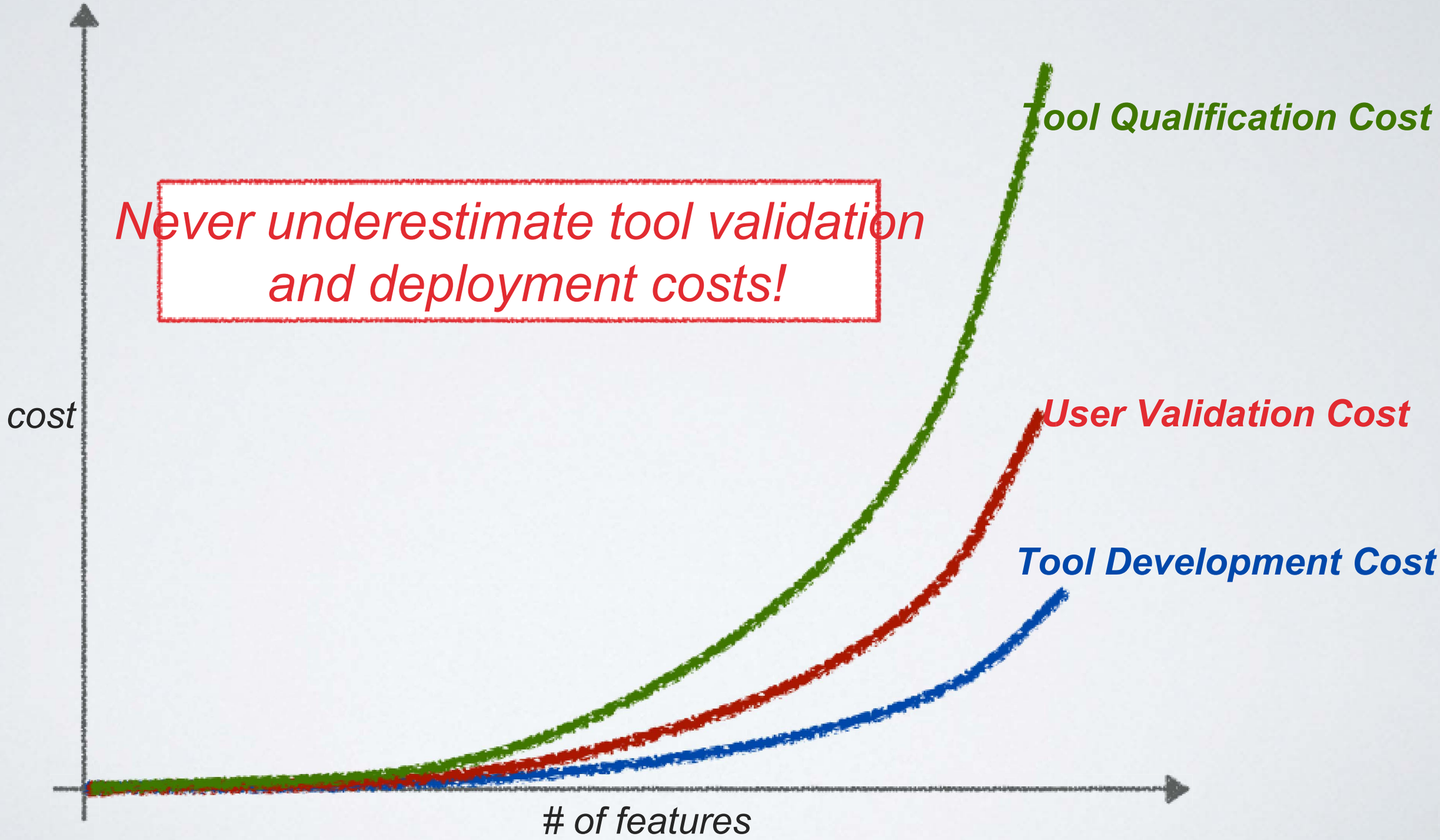
Src-to-obj traceability
Barco, MOSArt, 2010

CodePeer DO-178B Ver. Tool,
Utas UK, A400M, 2014

WHY?

The End User Forgets That Tools are Generally Off-The-Shelf Products

Never underestimate tool validation and deployment costs!



Example: add a feature to a Code Generator

DO-178C TQL1 style

"We need a code generation switch called --wrap-state that encapsulates persistent variables into a struct ."

Tool User

Tool Developer Activities

1 new command line option

3 + N new requirements (N ≈ 100)

N new testcases

500 SLOC to develop, trace and review

Review qualified interface

Re-execute all tests and review results

Re-perform QA

...

Tool User Activities

Review and asses new requirements

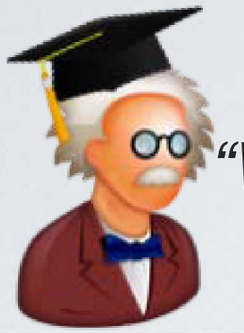
Review new tool qualified interface

Update internal procedures

Develop, review and validate new use cases

...

Align Stakeholders' Interests



"We need more formal tools!"

Academic

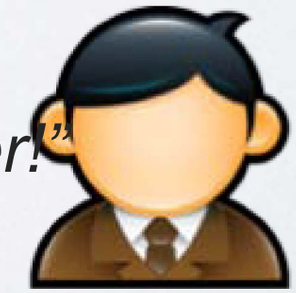
"We need tools that are cheaper to develop and qualify!"

Tool Provider

We need to understand how tools work and assess their qualifications!

QA Manager

"We need better tools that can be used by any engineer!"



Tool Manager

We Stop Thinking in terms of Return on Investment (ROI)

*“Tool Qualification is always a pointless waste
of time and resources!”*

Tool Provider

*“I need a Qualified Tool, no matter what
ven if I am not gaining certification credit from it)!”*

Tool User

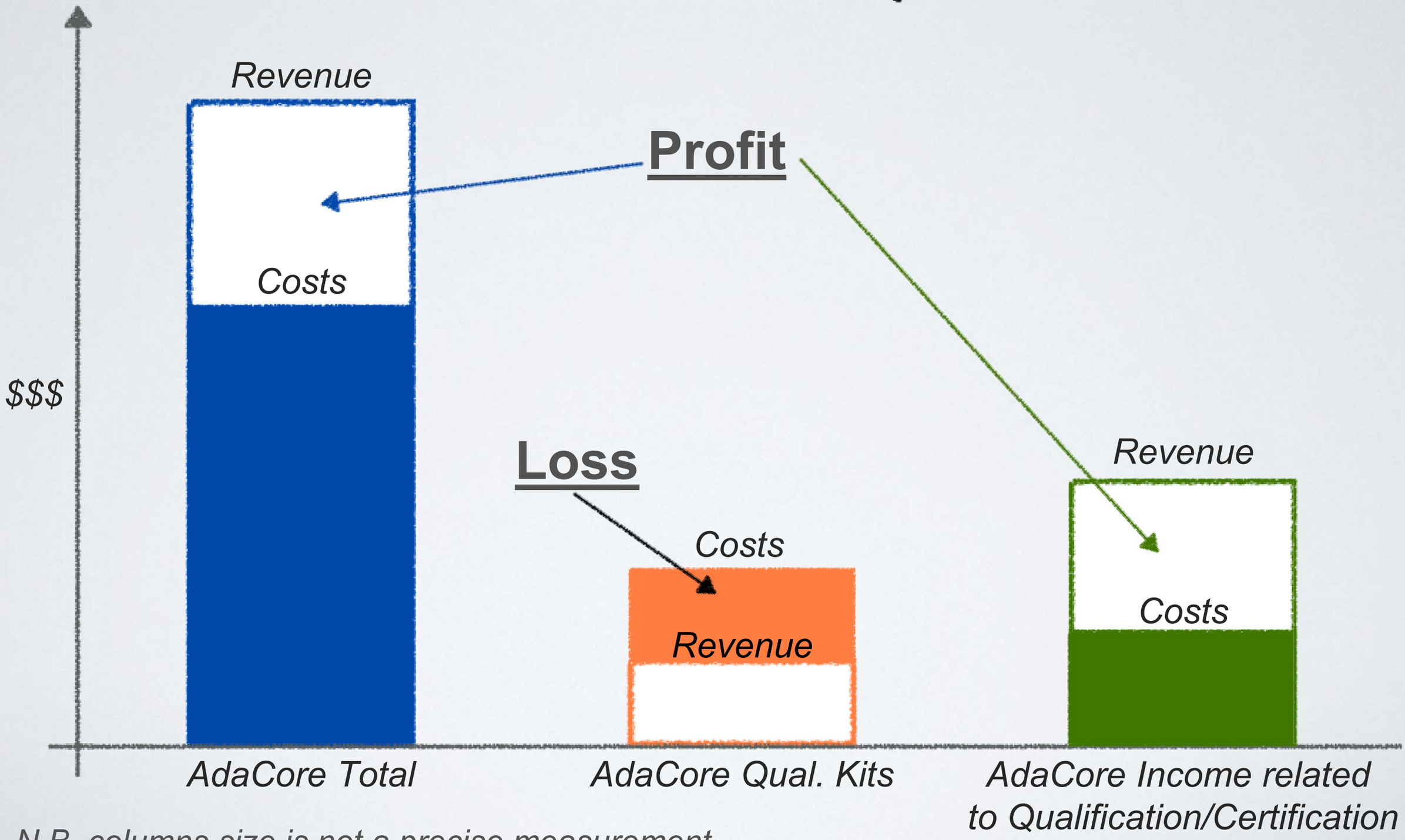
Main Sources of Waste in Tool Qualification

- User Forgets that Tools are COTS
- Uncontrolled Innovation: non-aligned interests
- We Forget about Return On Investment

The Economic Engine of Tool Qualification

Where the Profit is Coming From

a Tool Provider Perspective



N.B. columns size is not a precise measurement

Where the Profit is Coming From

a Tool Provider Perspective

Let's be clear - Qualification Kits are quite costly to produce and keep up to date, and generate relatively low revenue.

A Tool Provider cannot scale just by selling them

They bring very significant added value to customers

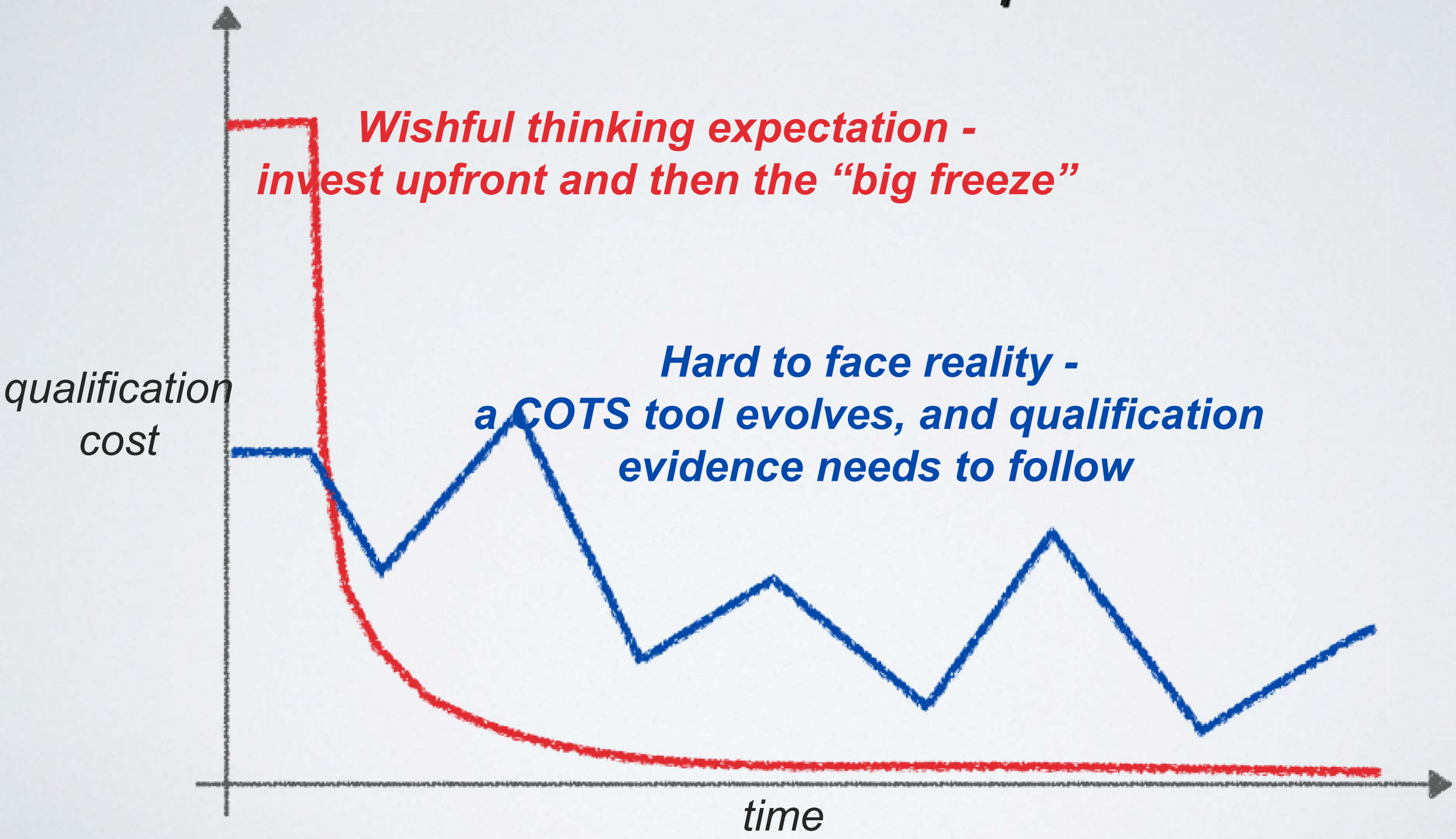
And it is not their core business to produce and maintain them

Qualification Kits are true enablers for selling other products

We need always up-to-date qualification kits

The Cost of Tool Qualification

a Tool Provider Perspective



The Need for a New Focus

from purely technical to operational excellence

<u>Today:</u> the ***"Big Freeze"***: invest upfront on tech and qualification kit, followed by slow, on-demand, evolution

"So you found a bug in our qualified tool?
Well, here you have a workaround: just do not use that feature!"

<u>Tomorrow:</u> a continuous, lean improvement of tool capabilities and qualification evidence

"So you found a bug in our qualified tool?
Well, here you have a ***corrective patch*** *plus an* ***impact analysis report****!"*

INCREASING

operational excellence

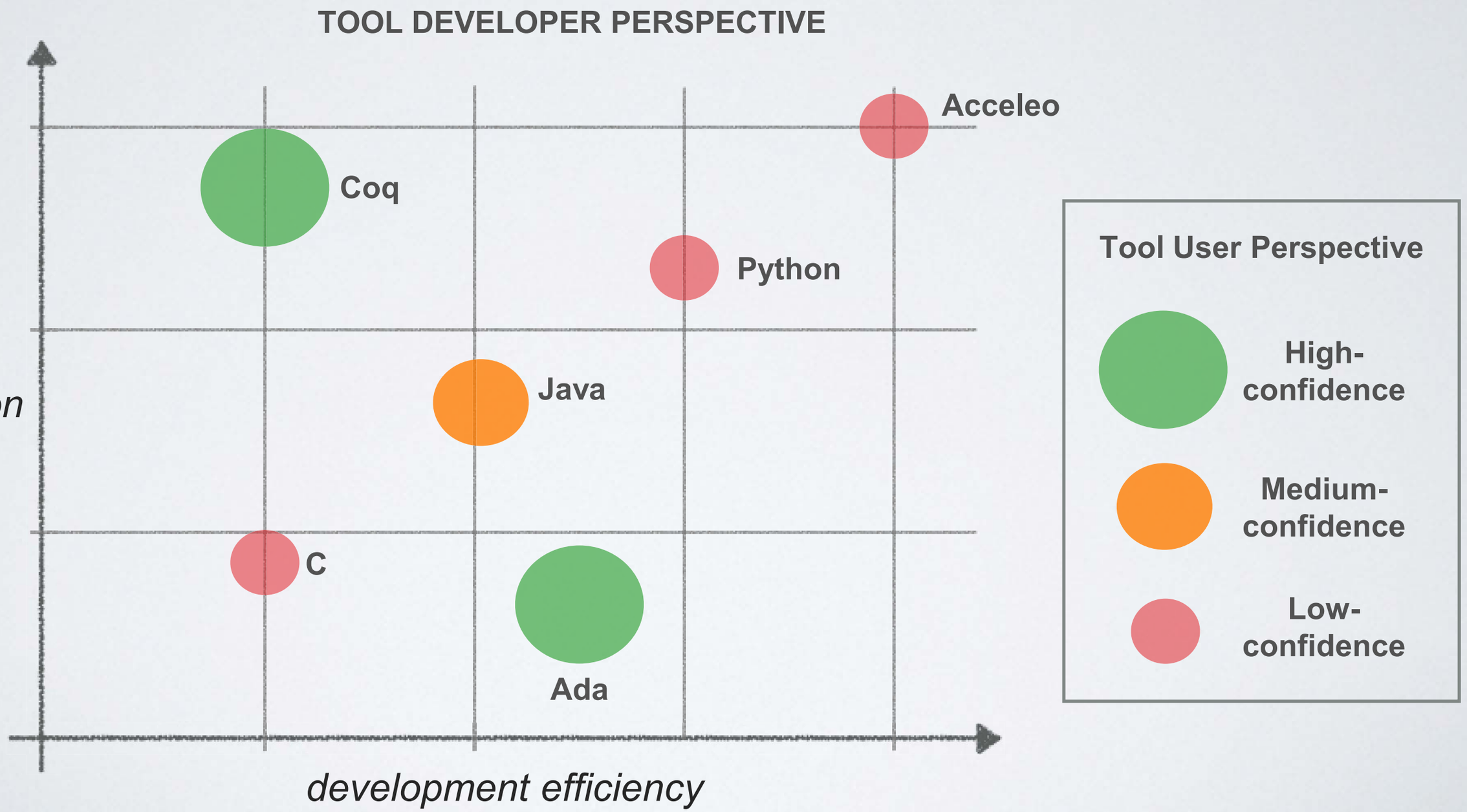
Increasing operational excellence

- Align interests by choosing the right technology
- Decrease costs by using Open-Source Technologies
- Improve your process by doing Lean & Agile Qualification

Choosing the right technology

Aligning interests

Case study: a code generator, to be qualified as per DO-178C TQL1



Using Open/Free Technologies

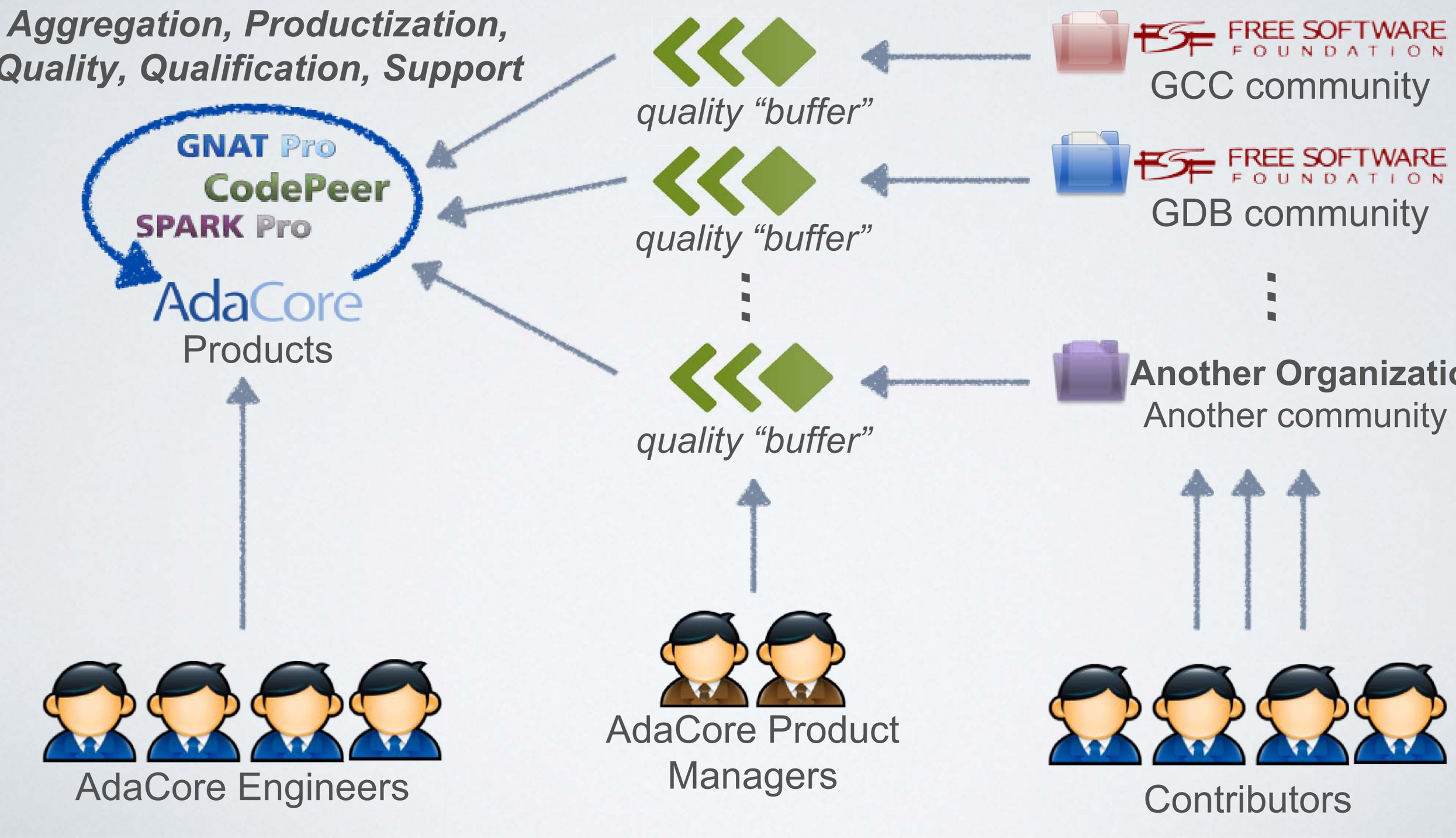
A little bit of terminology…

***Freely Licensed* software**
Software distributed with a license that allows to study, change and redistribute its source code

***Open Source* Community**
A way to manage the development of software with multiple stakeholders

The opposite of *Free* is *"proprietary,"* not *"commercial."*
AdaCore sells *Commercial*, *Freely Licensed* Qualifiable Toolsets

AdaCore Process for Open Source



Qualified, Commercial Freely Licensed Software is Possible

AdaCore

Runtime: DO-178B/C level A, EN-50128 SIL3/4, ECSS-E-ST-40C level B

Compiler: DO-178B/C level A Src-to-obj traceability, EN-50128 T3

Verification tools: DO-178B/C, EN-50128 T2

Avionics DO-178B/C	Railway EN-50128	Space ECSS-E-ST-40C
Airbus	Alstom	Astrium
Eurocopter	Ansaldo	Thales Alenia Space
General Electric	Invesys	
Honeywell	Siemens	
Rockwell Collins		
Thales		

Benefits of Qualified, Commercial Freely Licensed Software

Tool Provider

- Invests on products, not core technology
- Disrupts technology AND business model
- Innovate, always
- Track public repository
- Entry barrier is product/support quality, not vendor lock in
- Promote long-term clients engagement

Industrial Users

- No vendor lock in
- Free access to sources (certif. / qualif.)
- Long-term guarantee of tool sustainability
- Guarantee of controlled innovation

The software distribution license (free or not)

has no impact on tool qualification

The use of open-source technology requires an investment in

“qualifying” external contribution anyway

Safety-related qualification is “just” another step in the same direction

Lean & Agile Tool Qualification

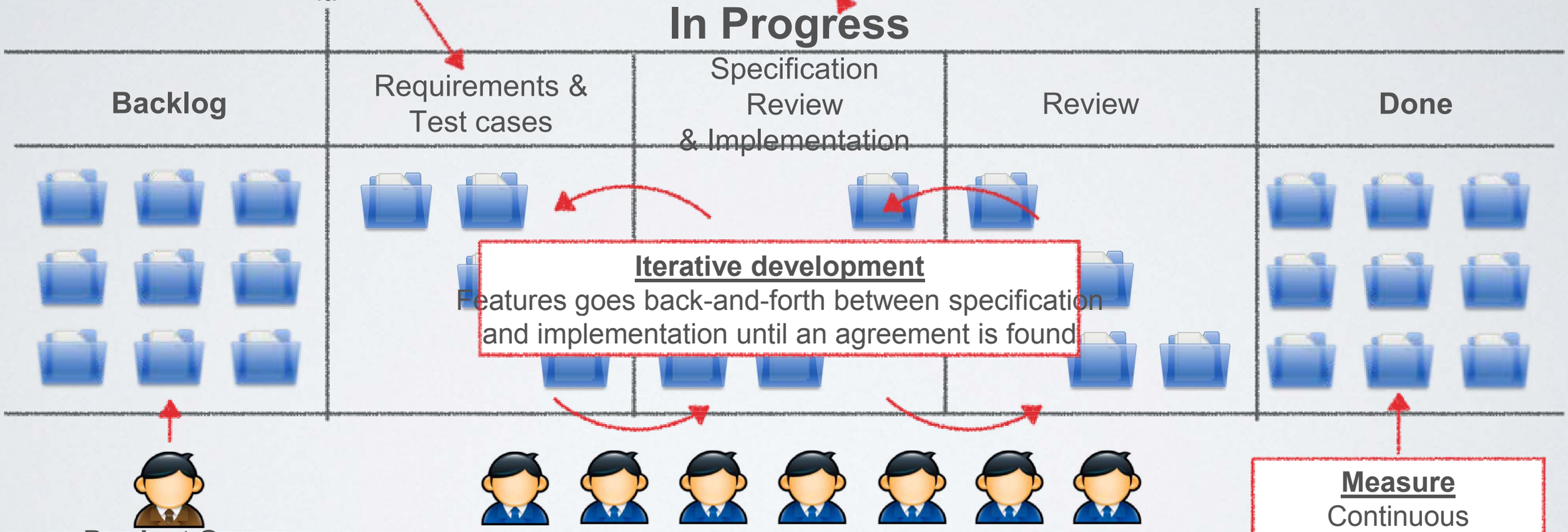
AdaCore Main Problem

- Two releases per year (major + minor)
- Customers on both legacy (frozen toolchain) and future programs
- Freely Licensed Software Vendors: need to innovate to retain customers
- Including qualification material

Lean & Agile Development

Test-driven development
Requirements and tests are developed within the same process by the same person.
No feature is ever implemented if there is not a test for it.

Incremental development
At any time, multiple features are “In Progress”, at different steps (minimize backlog and work-in-progress)



Iterative development
Features goes back-and-forth between specification and implementation until an agreement is found

Product Owner
A single person is in charge of both long term product strategy and day-to-day technical execution

Developers
Every developer is involved in both specification, implementation and review stages.

Measure
Continuous performance measurement

Highly Automated Quality Assurance and Configuration Management

CHALLENGES AHEAD

a tool provider perspective

Challenges Ahead
a Tool Provider Perspective

- Convergence of Safety Standards
- Effective Qualification of Development Toolchains
- Effective Qualification of Formal Tools
- Support for Semi-Frozen Branches of Qualified Tools

Convergence of safety standards

	DO-178C	EN-50128	ECSS-Q80*
Tool Specifications	Tool Operational Requirements	Can be a user guide, requirements, …	NO
Tool Validation	Requirement-driven testing	Can be testing, proven in use, …	NO
Configuration Management *(Tool developer side)*	YES	ISO-9000 or similar	NO
Quality Assurance *(Tool developer side)*	YES	ISO-9000 or similar	NO
Qualification entity	FAA/EASA	Independent Assessor	ESA
Impact of category on qualification cost	+++	+	zero

*Only de jure exception: automatic code generators. De facto, even code generators are not qualified.

Convergence of safety standards

Example: Compiler Qualification

- In DO-178, (aerospace) qualifying development tools is so hard that qualifying a compiler would have been impossible
  - Compiler qualification is in fact not required
    - CompCert is a great tool but it is **not** qualified accordingly to DO-178
- In EN-50128, (railway) qualifying a compiler as a T3 Tool takes a few weeks at most
  - As long as you know what you are doing

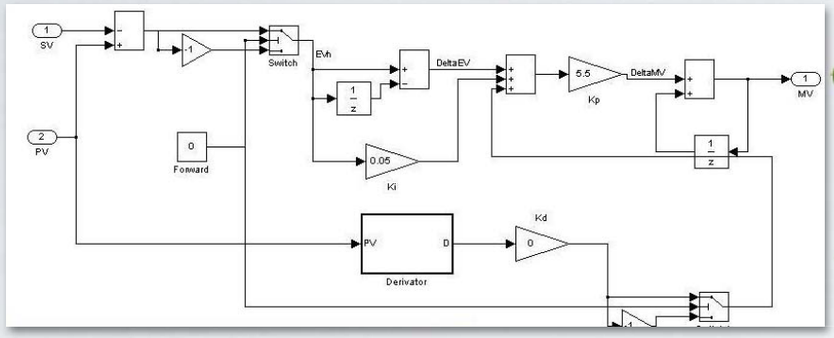
Convergence of safety standards

- DO-330 is the most comprehensive tool qualification document
- More emphasis on error impact analysis and mitigation techniques; what bad things can happen when the tool has a bug?
- Need to correlate tool category, certification credit, and qualification costs (tool qualification ROI) – rules to qualify a tool depend on whether its output actually "flies," and how much certification credit it provides
- Increasingly complex tools: need for toolchain qualification?

Camus et al.: "Tool Qualification in Multiple Domains: Status and Perspectives", ERTS 2014

Example: QGen Qualified Model Verification and Code Generator

a complete model verification and compilation **toolchain** for Simulink®



Proof of absence of run-time errors & safety/functional properties

Qualified Code Generator

Ada & MISRA C

GNAT Pro Safety-Critical

Validated Compiler

Effective Qualification Of Formal Tools

Domain	Standard	Last Version	Formal Methods for specification	Formal Methods for implementation
Avionics	DO-178, DO-333	2012	Applicable	Applicable
Automotive	ISO-26262	2011	Applicable	Applicable
Medical	IEC 62304	2006	Recommended	Recommended
Nuclear	IEC 60880	2006	Encouraged	Applicable
Railway	EN 50128	2011	Applicable	Recommended
Space	ECSS-Q-ST-80C	2009	Applicable	Applicable

Effective Qualification Of Formal Tools

- They offer 100% guarantee - as long as assumptions are verified!
- How to ensure
  - Model is representative/adequate
  - Assumptions on environment/integration are verified
- Several methods/tools: a common approach for tool qualification?

Working group on “Theorem Proving in Certification” since 2010

Draft document soon available

Join tpcert@googlegroups.com

Ultimate Challenge: Semi-Frozen Branches of Qualified Tools

Critical Bug In the Hardware
Critical Issue In the Qualified Tool
…

Qualified Tool User Project Lifecycle

2 years later…

Tool User Freezes Development Environment

Qualified Tool Release History

ver. X.0 ver. X.1 ver. X.2 ver. Y.0 ver. Y.1 ver. Y.1

Semi-Frozen Branches of Qualified Tools: a service providing critical patches to frozen product versions with detailed impact analysis

TAKE HOME

messages

Take Home Messages

- **Tool Qualification has a cost**
  - For both the tool provider AND the tool user
  - This cost is exponential w.r.t. the complexity of the tool
- **Think about Return On Investment when qualifying a tool**
  - Tool provider: *“Is this qualification kit an enabler?”*
  - Tool user: *“Am I getting significant certification credit?”*

Take Home Messages

- **Qualification of Open-Source Tools**
  - Distribution license per se has no impact on qualification
  - You need to be VERY organized to collaborate with open communities
  - Your added value is in integration, validation, quality, support
- **Getting Things Done**
  - A lot to learn from modern development methods
  - We cannot do C*ontinuous Deployment*, but we can have a *DevOps-oriented lifecycle* with *Lean/Agile Development and Qualification*

Take Home Messages

- **Convergence of Safety Standards**
  - A direct relation between Tool Category, Tool Qualification Cost, and Certification Credit
  - We, as a community, need to measure our Return On Investment
- **Challenges Ahead**
  - Example of Effective Qualification of Development Toolchains: QGen Model Verifier and Code Generator
  - Supporting semi-frozen branches of qualified tools

thanks!

Tucker Taft taft@adacore.com
Matteo Bordin, bordin@adacore.com

AdaCore