# Open Source in Functional Safety products

**Nicolás Martín-Vivaldi**

2018-05-22

addalot
QUALITY IMPROVEMENT

# Agenda

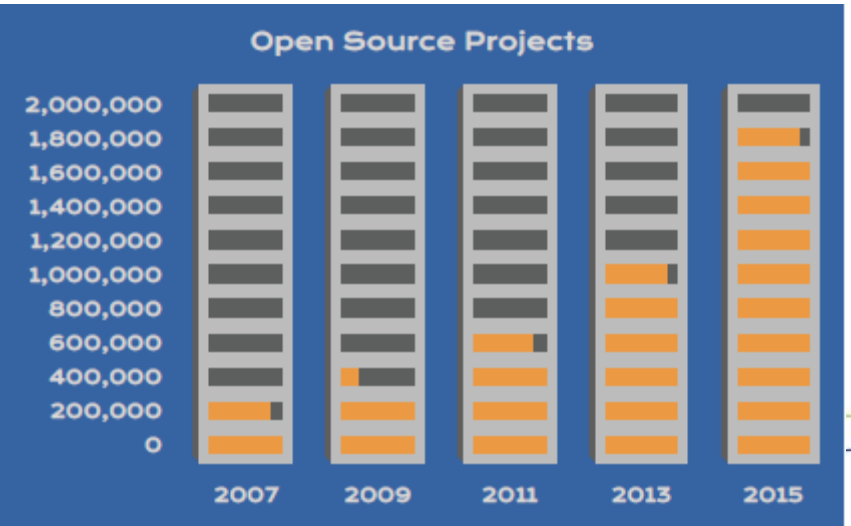
- Open Source
- Open Source and Functional Safety
- Handbook for Industrial Open Source

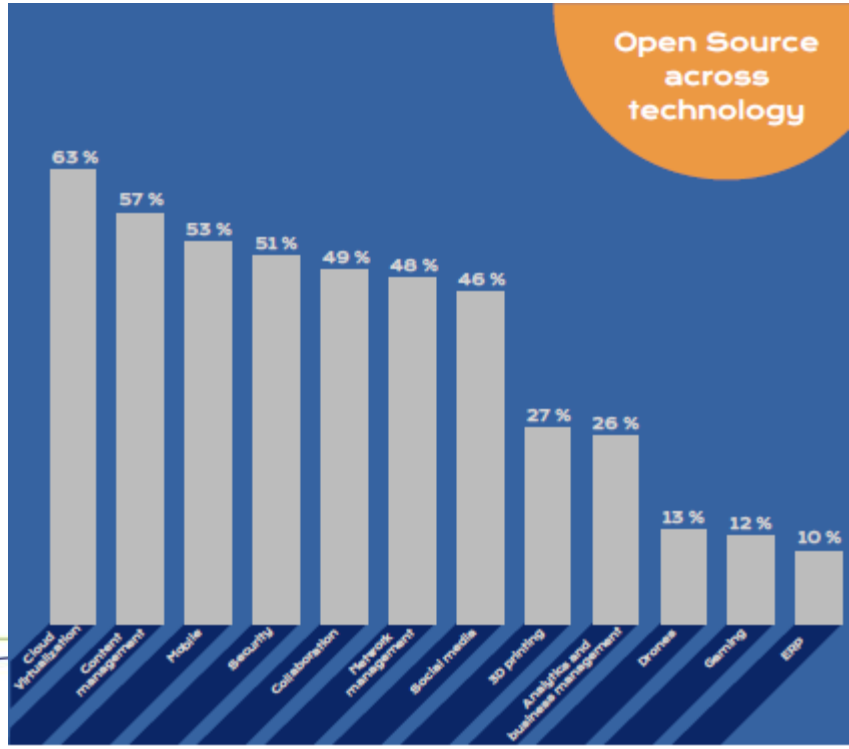



addalot
QUALITY IMPROVEMENT

# Open Source: *Not new – but timing is right*

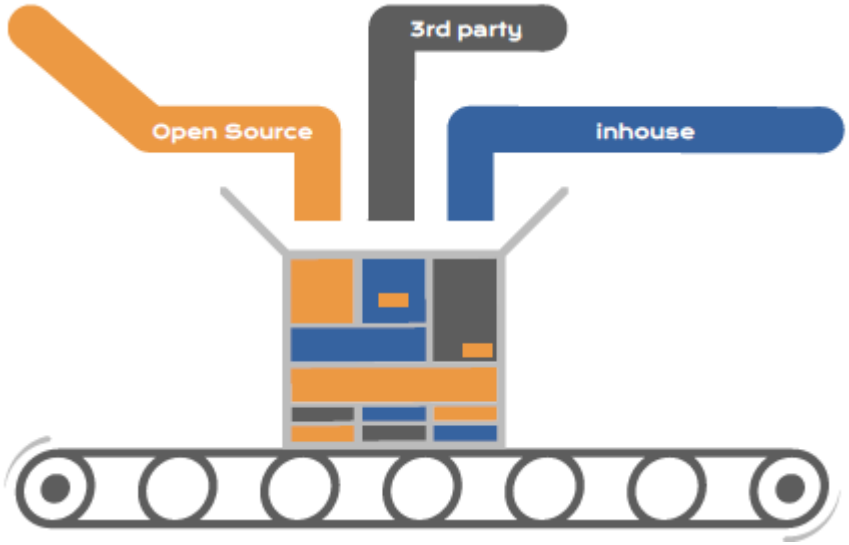
- Has been around for years, but recently has the usage accelerated
- Now in most domains
- Several facts driving the increased usage of OSS:
  - Global development awareness and access
  - Merge of domains, eg connectivity technology with previously closed applications
  - Increased demand for reduced lead-times and development cost
  - Snowball effect, The big players are doing it, so now everyone else wants to get involved.



# From development to integration

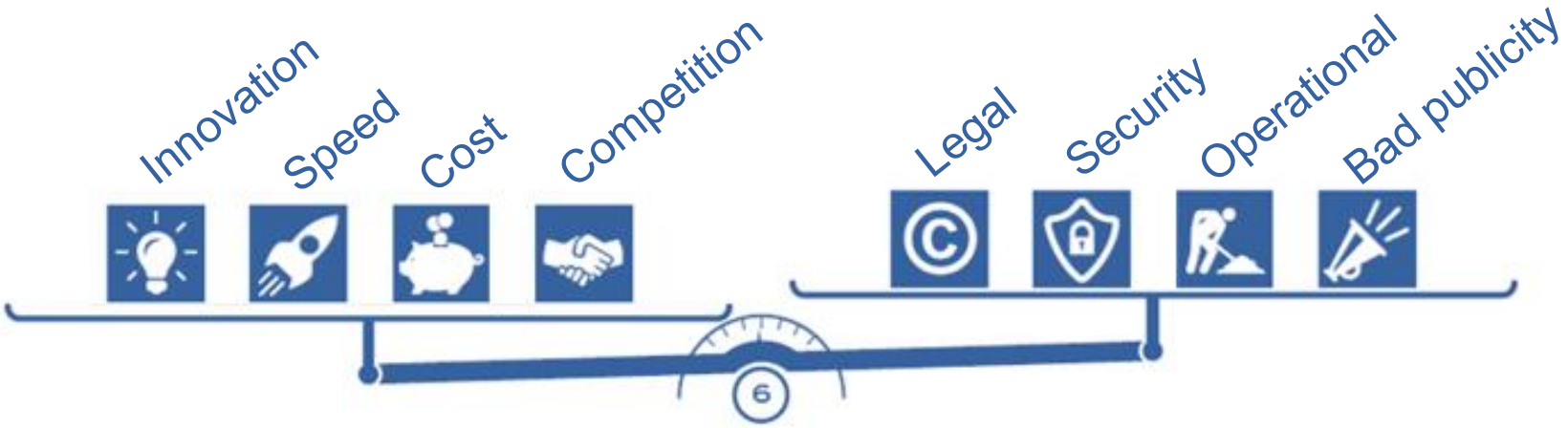
- Used to be primarily In-house with some limited additions
- Today a majority(*) of application are Open source & Third party (*) Gartner






addalot QUALITY IMPROVEMENT

# Benfits vs Challenges



# Business aspects

- Open ≠ Free
  - Developed for free? ➔ Majority of OSS developers are paid
  - Free usage? ➔ Free License fee but Governance costs! (support, maintenance, …)

- Open Source business models
  - Extended model (Support, Services, “Open core”)
  - Indirect model (HW)
  - Asymmetric model (Data, Advertisement)

- Business strategies often involve Open Source based eco-system that enable additional revenue streams

# Examples






addalot
QUALITY IMPROVEMENT

# Open Source in Functional Safety






addalot QUALITY IMPROVEMENT

# Different levels of usage

- Tool chain (Validation needed)
- Non safety features (supporting library)
- Part of core product (OS)
- Part of safety function

# How to handle?


- Same as for 3rd party products

- Difference between models
  - 26262: Qualification of a software component
  - 62304: SOUP – **S**oftware **O**f **U**nknown **P**rovinence
  - 61508: Proven in use / assessment of non-compliant development



addalot QUALITY IMPROVEMENT

# Expectations 1(2)

## 26262 – Qualification of SW

- General
- Planning
- Qualification
  - Specification (req's)
  - Evidence of compliance (verification)
  - Documentation of
- Verification
  - Verify qualification result
  - Intended use
- Work products
  - SW component documentation
  - SW component qualification report
  - Safety plan (updated)

## 62304 - SOUP

- Software requirements: The manufacturer shall describe what requirements (functions or non-functional) are necessary to have the SOUP work.
- Architecture: The manufacturer shall define the software architecture to have the SOUP work in appropriate conditions.
- Maintenance: The manufacturer shall monitor the SOUP lifecycle: patches, new versions…
- Risk analysis: It is mandatory to do a risk analysis related to the SOUP.



addalot QUALITY IMPROVEMENT

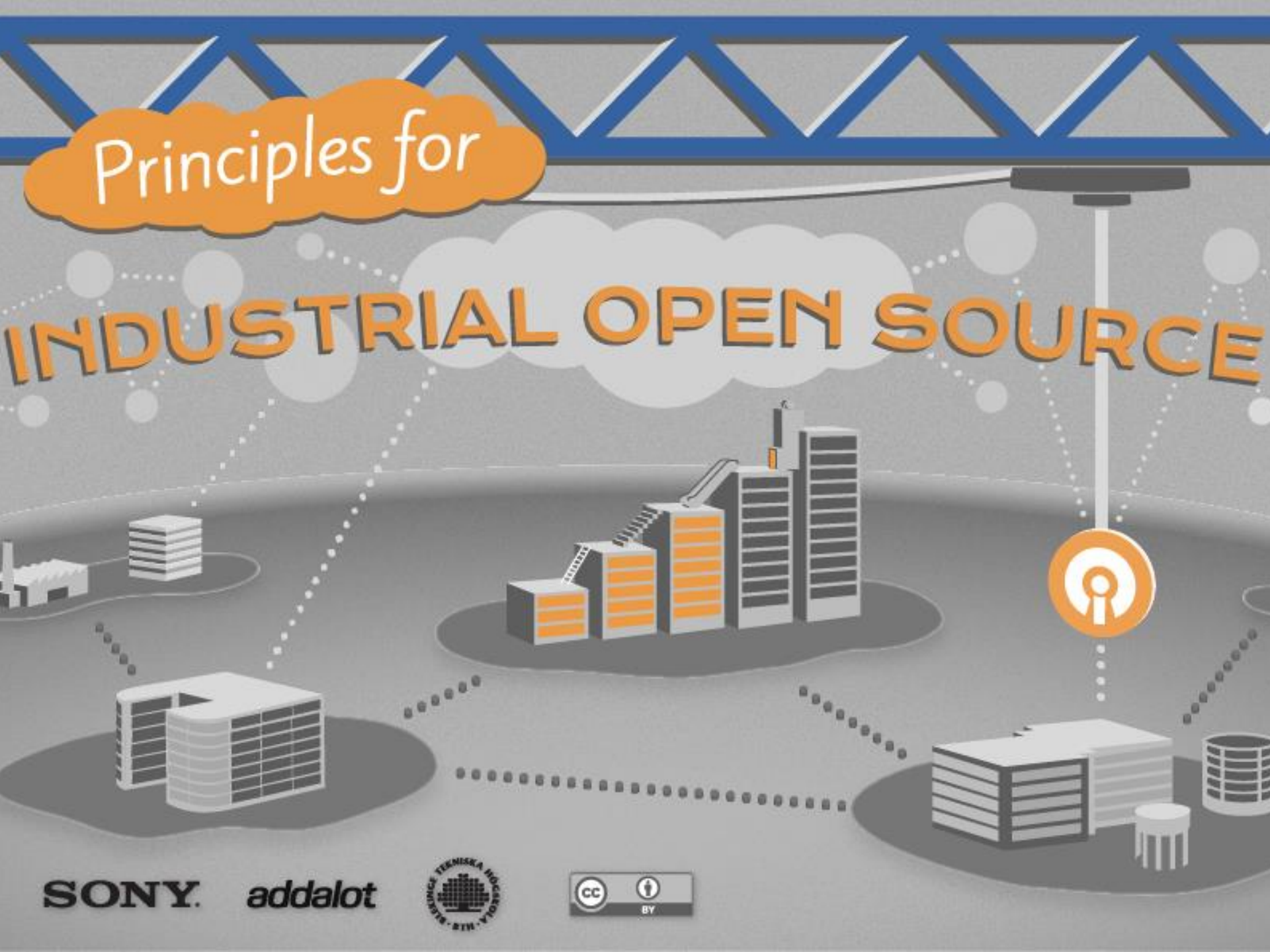
# Expectations 1(2)

**61508**

- **7.4.2.12** Where a pre-existing software element is reused to implement all or part of a safety function, the element shall meet both requirements a) and b) below for systematic safety integrity:
  - compliant development. Compliance with the requirements of this standard
  - proven in use
  - assessment of non-compliant development.

# 61508 - Assessment

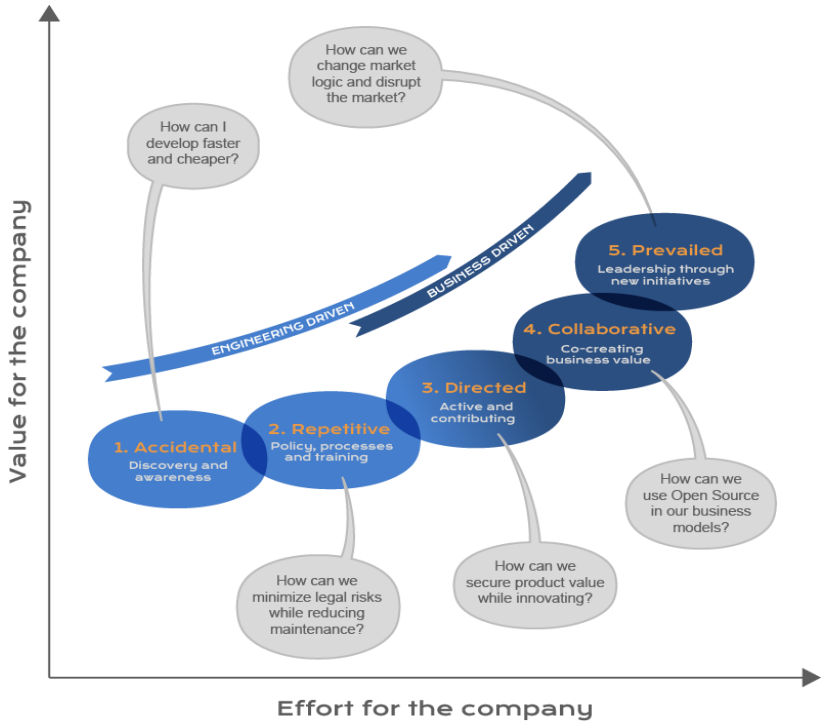
A. The software safety requirements specification for the element in its new application shallbe documented to the same degree of precision as would be required by this standard for any safety related element of the same systematic capability.
B. The justification for use of a software element shall provide evidence that the desirable safety properties specified in the referenced subclauses (i.e……)
C. The element's design shall be documented to a degree of precision, sufficient to provide evidence of compliance with the requirement specification and the required systematic capability.
D. The evidence shall cover the software's integration with the hardware.
E. There shall be evidence that the element has been subject to verification and validation using a systematic approach with documented testing and review of all parts of the element's design and code.
F. Where the software element provides functions which are not required in the safety related system, then evidence shall be provided that the unwanted functions will not prevent the E/E/PE system from meeting its safety requirements.
G. There shall be evidence that all credible failure mechanisms of the software element have been identified and that appropriate mitigation measures have been implemented.
H. The planning for use of the element shall identify the configuration of the software element, the software and hardware run-time environment and if necessary the configuration of the compilation / linking system.
I. The justification for use of the element shall be valid for only those applications which respect the assumptions made in the compliant item safety manual for the element


Principles for
INDUSTRIAL OPEN SOURCE
SONY
addalot
BLEKINGE TEKNISKA HÖGSKOLA · BTH ·
BY

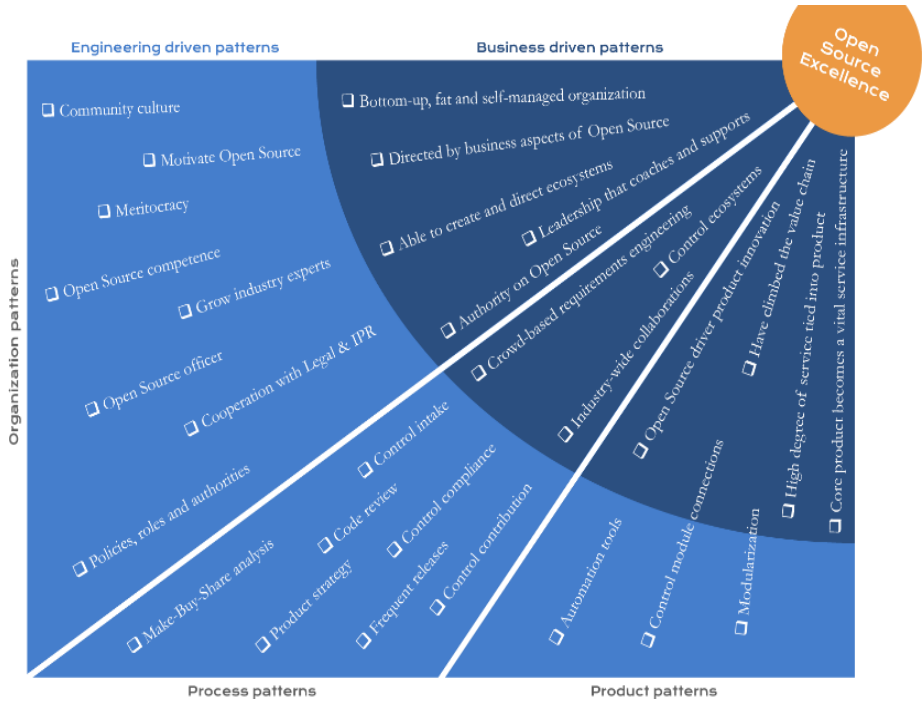
# Handbook: Principles for Industrial Open Source

Release 26/5-2018

## Part 1: The Journey




## Part 2: The Patterns








addalot QUALITY IMPROVEMENT

# Questions?


SWEDSOFT - Working group on Open Source (Sony, Scania, QLIK, …)



addalot QUALITY IMPROVEMENT

*"Because not all the smart people work for you"*

*Bill Joy co-founder of Sun Microsystems*

**Nicolas.Martin-Vivaldi@addalot.se**
**+46 706 800 521**

addalot
QUALITY IMPROVEMENT