ASGARD

9TH COMMUNITY OF USERS ON SAFE, SECURE AND RESILIENT SOCIETIES

WORKSHOP ON CYBERCRIME

6th DECEMBER 2017

Seán Gaines

Director of International Projects

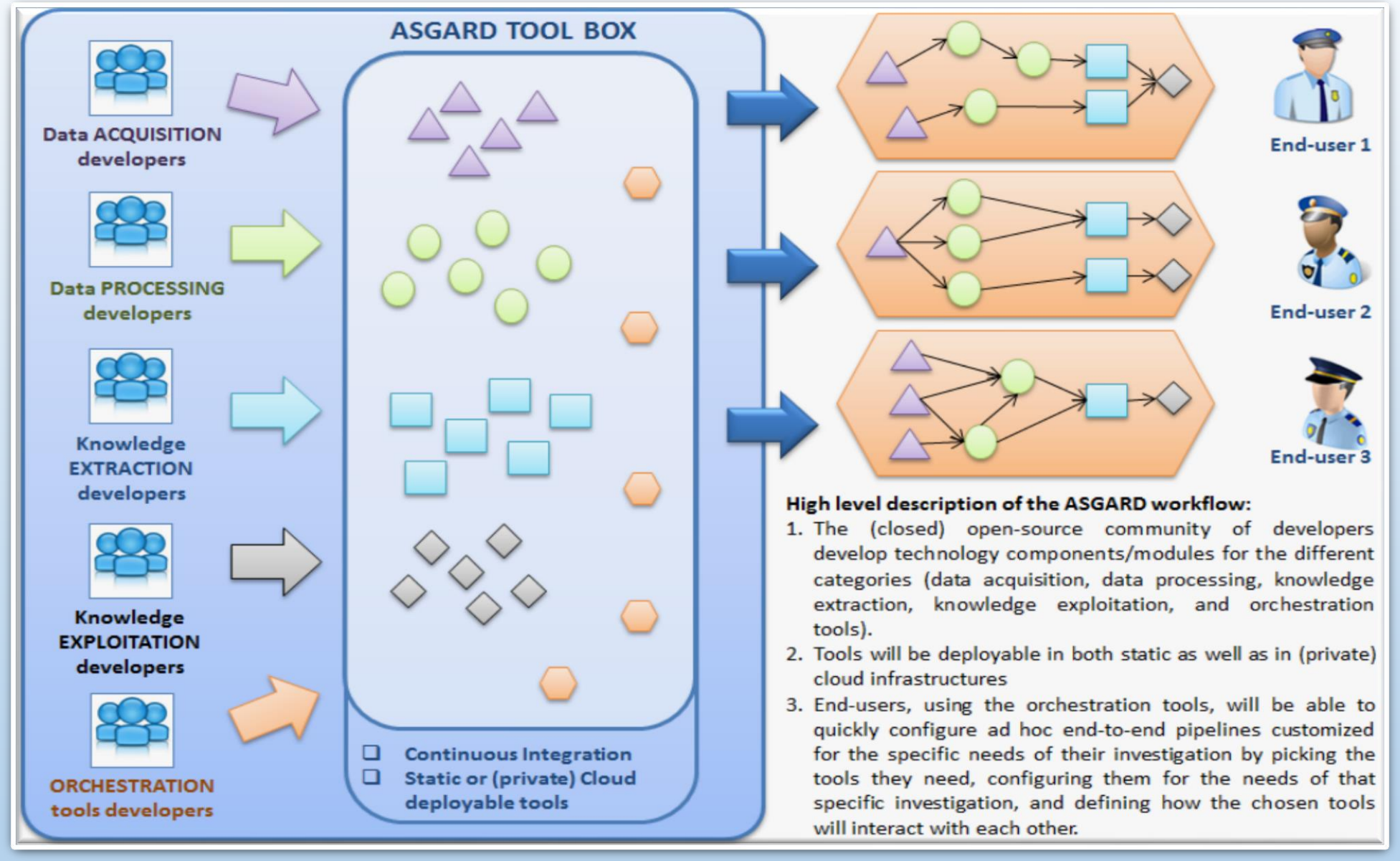
Vicomtech-IK4

Project Goal

- The ASGARD project aims at **providing LEAs with Technological Autonomy** by creating a long lasting and **sustainable community of LEAs, research and development, and industrial actors**, focused on a set of **tools and techniques**, that facilitate effective collaboration in order to **define, develop, share, and evolve open source data analytic technologies** that will **help LEAs prevent and fight against crime and terrorism**.

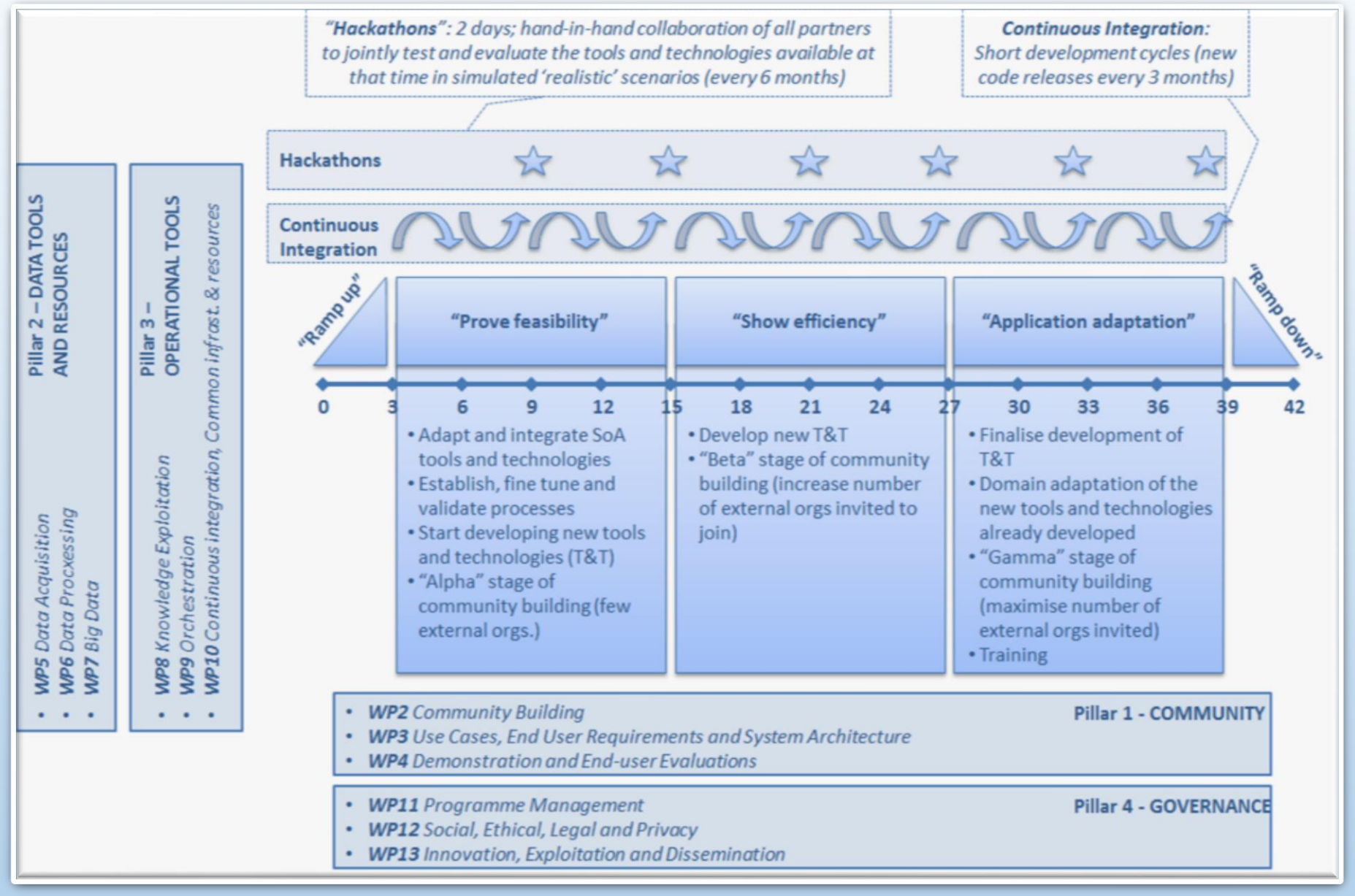
Project Strategy

- **Interoperability**: Develop easy-to-use, interoperable sets of tools which **complement LEAs' current systems**.
- **Technological breakthrough**: Build upon the work in prior related projects, ground-breaking technologies tackling LEAs prioritised needs in the fields of **multimedia big data acquisition, processing, fusion, mining, visualisation and collaboration**.
- **Agile**: Modern **continuous development and integration** methodologies and **short development cycles** to ensure the LEAs in the project have **early and frequent access to the project results** (at least 6 times during the project) so that they can **provide prompt feedback to re-prioritise the work plan if needed**


ASGARD TOOL BOX
Data ACQUISITION developers
Data PROCESSING developers
Knowledge EXTRACTION developers
Knowledge EXPLOITATION developers
ORCHESTRATION tools developers
Continuous Integration
Static or (private) Cloud deployable tools
End-user 1
End-user 2
End-user 3
High level description of the ASGARD workflow:
1. The (closed) open-source community of developers develop technology components/modules for the different categories (data acquisition, data processing, knowledge extraction, knowledge exploitation, and orchestration tools).
2. Tools will be deployable in both static as well as in (private) cloud infrastructures
3. End-users, using the orchestration tools, will be able to quickly configure ad hoc end-to-end pipelines customized for the specific needs of their investigation by picking the tools they need, configuring them for the needs of that specific investigation, and defining how the chosen tools will interact with each other.

Project Strategy

- **Fluid, Frequent, and Fruitful collaboration** between all stakeholders, including short development cycles and face-to-face "**Hackathons**" **every 6 months**. After the hackathons **LEAs will be able to take the tools, deploy and test them in their own premises and with their own data** providing feedback to the ASGARD community.
- **Build the sustainable community** starting with a **large representation of the different stakeholders** in the strong ASGARD consortium.
- Definition and design of the solution based on (1) **forensic**, **intelligence** and **foresight** processes, (2) **end-user needs driven use cases and scenarios**, (3) **SoA technologies and beyond SoA** achievable challenges, and (4) **compliance with Social, Ethical, Legal, and Privacy** regulation and principles.


"Hackathons": 2 days; hand-in-hand collaboration of all partners to jointly test and evaluate the tools and technologies available at that time in simulated 'realistic' scenarios (every 6 months)
Continuous Integration: Short development cycles (new code releases every 3 months)
Hackathons
Continuous Integration
"Ramp up"
"Prove feasibility"
"Show efficiency"
"Application adaptation"
"Ramp down"
0 3 6 9 12 15 18 21 24 27 30 33 36 39 42
• Adapt and integrate SoA tools and technologies
• Establish, fine tune and validate processes
• Start developing new tools and technologies (T&T)
• "Alpha" stage of community building (few external orgs.)
• Develop new T&T
• "Beta" stage of community building (increase number of external orgs invited to join)
• Finalise development of T&T
• Domain adaptation of the new tools and technologies already developed
• "Gamma" stage of community building (maximise number of external orgs invited)
• Training
Pillar 2 – DATA TOOLS AND RESOURCES
• WP5 Data Acquisition
• WP6 Data Processing
• WP7 Big Data
Pillar 3 – OPERATIONAL TOOLS
• WP8 Knowledge Exploitation
• WP9 Orchestration
• WP10 Continuous integration, Common infrast. & resources
• WP2 Community Building
• WP3 Use Cases, End User Requirements and System Architecture
• WP4 Demonstration and End-user Evaluations
Pillar 1 - COMMUNITY
• WP11 Programme Management
• WP12 Social, Ethical, Legal and Privacy
• WP13 Innovation, Exploitation and Dissemination
Pillar 4 - GOVERNANCE

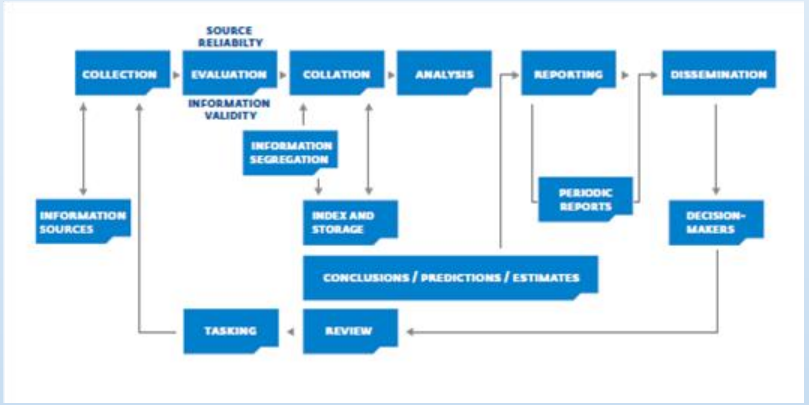
Multidisciplinary collaboration > how to make it possible in practice

- **Collaboration between LEA, industry and research organisations is not an easy task**, there are multiple obstacles and barriers.
- In the ASGARD project **we have found an effective and efficient way that makes possible in practice** this collaboration.
- Current focus and challenge is in breaking with tradition **on the definition and prioritisation of the end-user requirements and system specifications**.

Definition and prioritisation of end-user requirements and system specifications

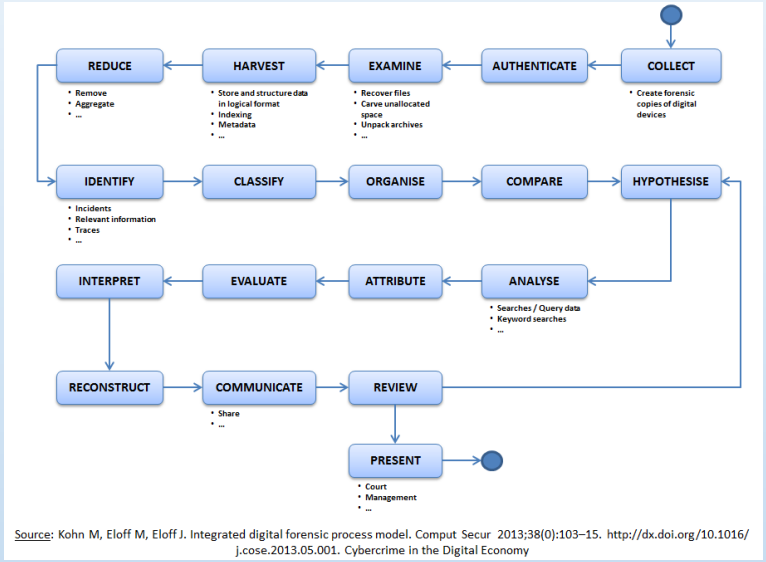
- **The ASGARD project was designed to be agile**, with technical partners **releasing tools and solutions to LEA partners every 6 months**, so that they can use, test, evaluate… and provide feedback that serves as an input for the plan-of-action of the following development cycles.
- The goal of the project is to **build a sustainable multidisciplinary community** which will **provide LEAs on a regular basis with novel tools and solutions** to help them increase their technological autonomy.
- **End-user requirements evolve continuously** and they have to be handled accordingly.
- The ASGARD project has **already established the basis of how to define, prioritise, and translate into system specifications** these requirements.

Starting by agreeing on which reference common process model(s) to use



Ref Frontex, 2012

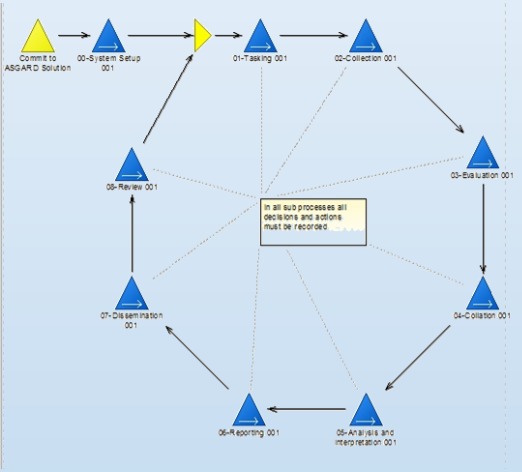
+



Source: Kohn M, Eloff M, Eloff J. Integrated digital forensic process model. Comput Secur 2013;38(0):103–15. http://dx.doi.org/10.1016/j.cose.2013.05.001. Cybercrime in the Digital Economy

IDFPM Ref: Kohn, 2012

=



ASGARD Process Model

Noteworthy documents:

UN Criminal Intelligence Manual for Analysts
ISO/IEC 27043 - I*ncident investigation principles and processes*

Use Cases

Digital Investigations

Trafficking of Illicit Goods and Information

Movement of People

https://www.europol.europa.eu/crime-areas-and-trends/crime-areas

From Use Cases (3) to User Stories (35) to End-User requirements (+190)

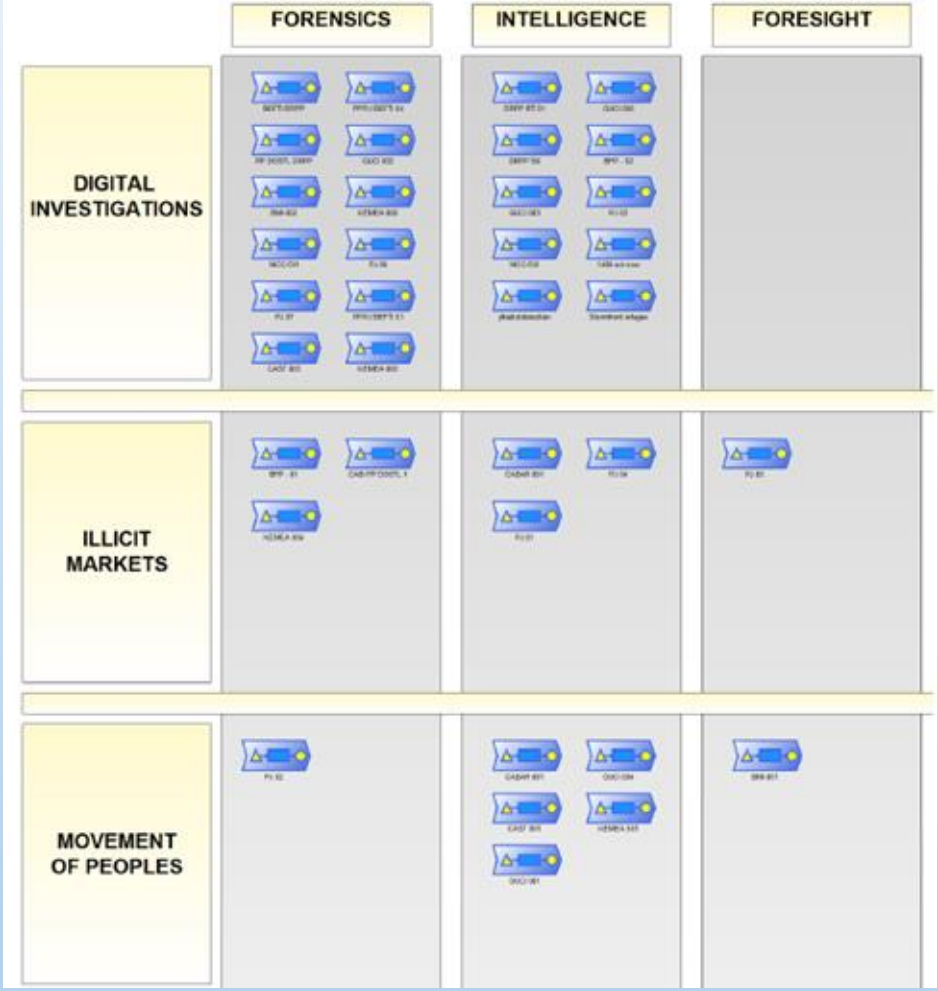
1. 3 umbrella use cases (topics) agreed by ASGARD LEAs
2. +35 specific user stories related to the 3 use cases and mapped to the different phases/stages of the agreed common process model
   - Including definition of the process, identification of legacy tools currently being used for each step of the process and, and of areas of improvement
3. Extracted +190 specific end-user requirements out of the 35 user stories (also mapped to the different phases of the common process model)

Processes

- 3 different processes used
  - Forensics
  - Intelligence
  - Foresight
- Models shown earlier were used to fit to these processes
- Much overlap between the processes – especially forensics and intelligence
- Many investigations will involve more than one of these processes at some point

Clustering User Stories

- The user stories were grouped by Use Case and Process
- The majority of stories were in the Digital Investigations Use Case and either the Forensics or Intelligence Process
- Can see the areas where we could add more user stories at a later date if required
- Some user stories actually cover more than one process



Analysis of User Stories

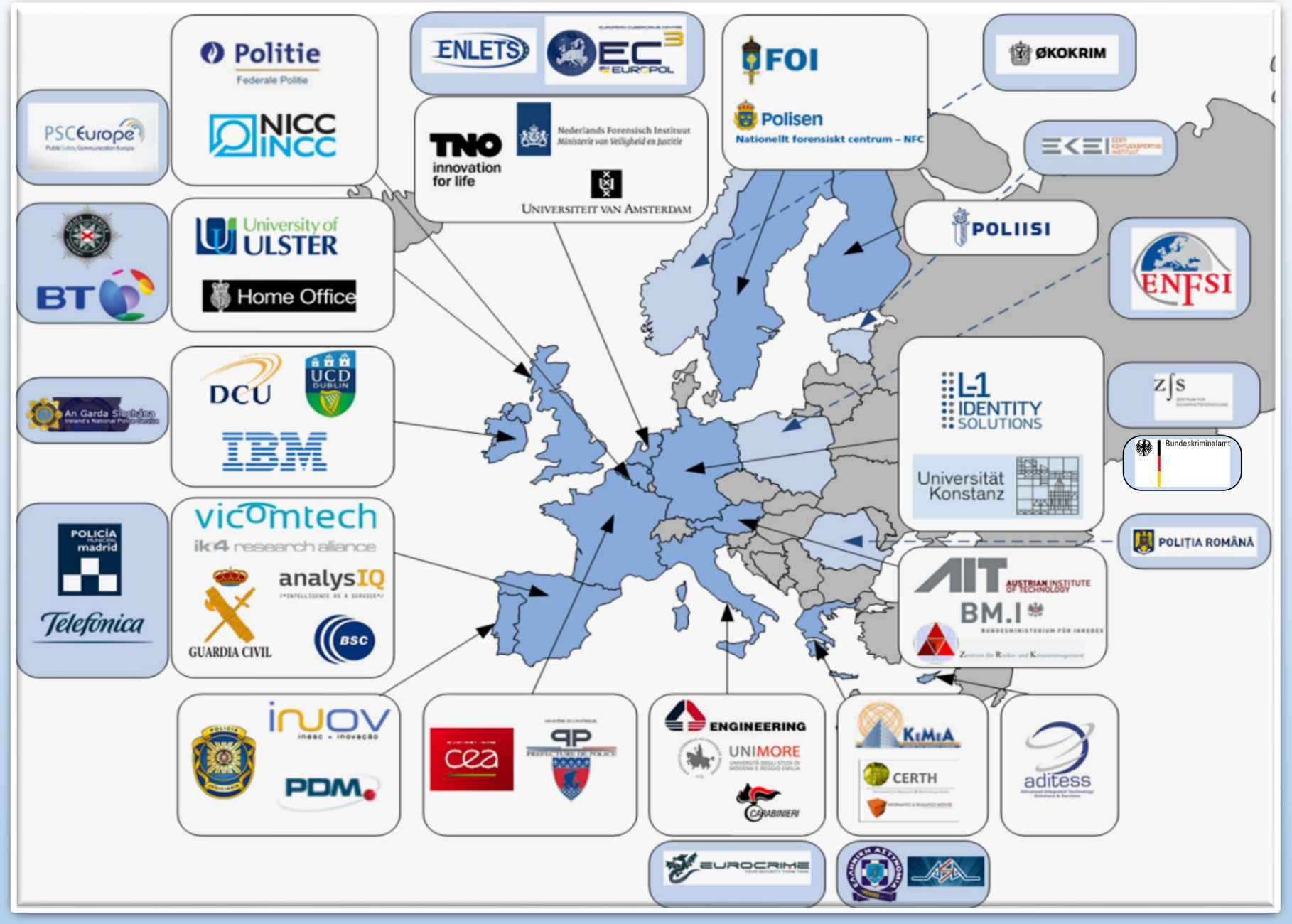
- Many common themes emerging
  - Device forensics
  - "Live" forensics (servers, RAM, cloud etc.)
  - Open Source Information Gathering (social media, forums etc.)
  - CCTV
- Lots of similar processes amongst LEAs and similar tools used
- Lots of similar issues faced too

User Requirements

- User Requirements taken from user stories
- Lots of interaction with LEAs to ensure we fully understood the requirements
- Currently they are quite high level but more detail will be added as the project goes on
- Iterative – new version after each Hackathon
- Each requirement given an LEA priority and a Technical feasibility to help define development scope

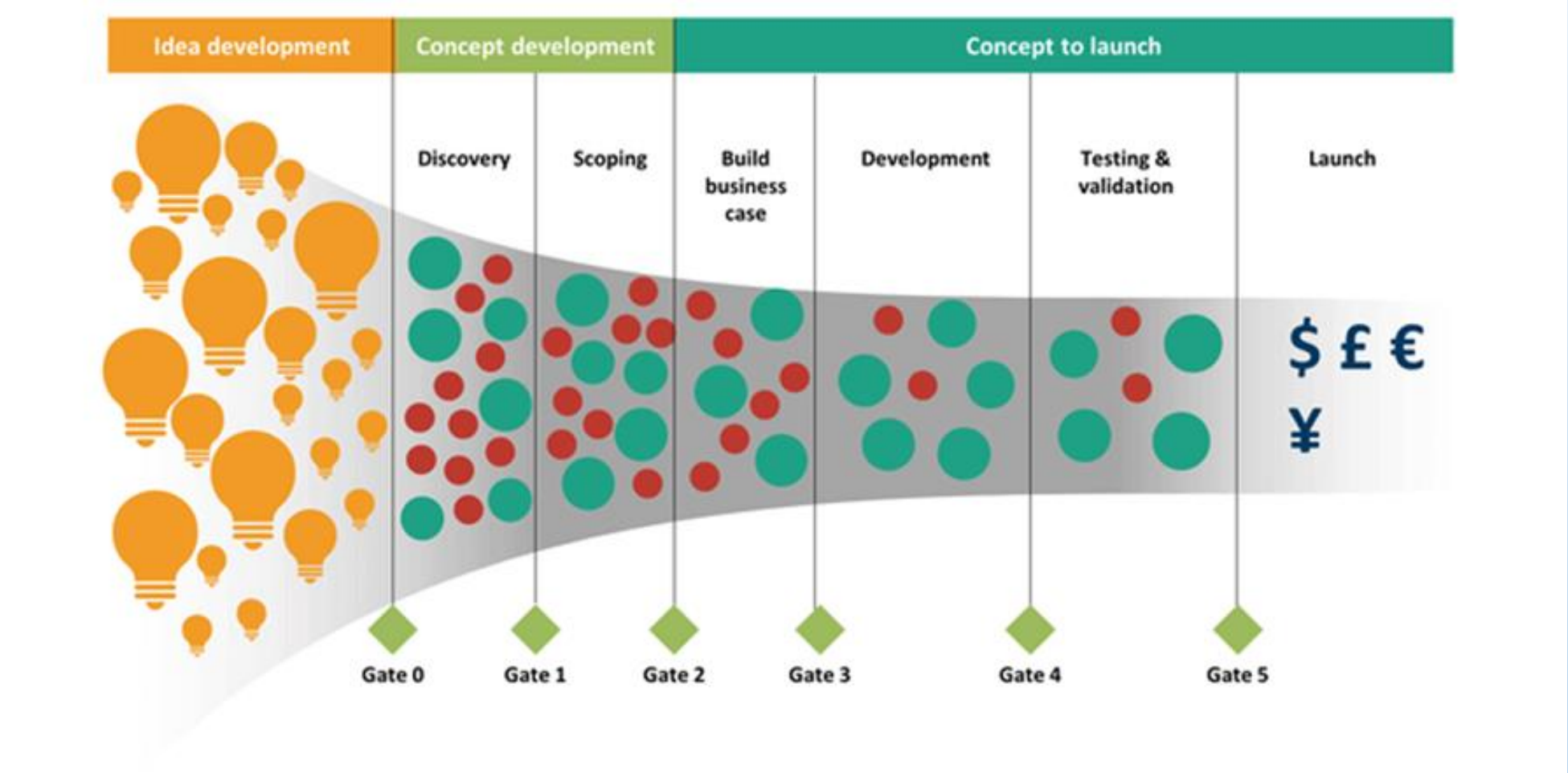
Roles

- We spoke to LEAs to see who was performing the activities in their scenarios
- We noticed there are many similarities between LEAs with regards to the roles they employ (not surprisingly)
- Defined a set of roles for the ASGARD system – for some LEAs one person may perform many roles
- Assigned each user requirement a role (or number of roles) to which the requirement is applicable


Politie
Federale Politie
NICC INCC
PSCEurope
ENLETS
EC3 EUROPOL
TNO innovation for life
Nederlands Forensisch Instituut
Ministerie van Veiligheid en Justitie
Universiteit van Amsterdam
FOI
Polisen
Nationellt forensiskt centrum – NFC
ØKOKRIM
EKEI
POLIISI
ENFSI
BT
University of ULSTER
Home Office
An Garda Síochána
DCU
UCD DUBLIN
IBM
L-1 IDENTITY SOLUTIONS
Universität Konstanz
ZfS
Bundeskriminalamt
POLIȚIA ROMÂNĂ
POLICÍA madrid
Telefónica
vicomtech
ik4 research alliance
analysIQ
GUARDIA CIVIL
BSC
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
BM.I
inov inesc inovação
PDM
cea
PREFECTURE OF POLICE
ENGINEERING
UNIMORE
CARABINIERI
KEMEA
CERTH
aditess
EUROCRIME

Innovation

- Funnel and Stage Gates



Innovation Management

- **Core process** in an organisation
- Innovation and generation of knowledge is **cyclical**
- Often managed as any other **project management task**
- Innovation occurs as an **interaction** between **actors**
- Open Innovation: Requires internal and external actors
- In innovation: Research **pushes** to market, market **pulls** from research

The Goals of innovation are:

- Product innovation **excellence**
- Product **leadership**
- **Accountability**
- **High-performance teams**
- Customer/market focus
- Robust solutions
- Alignment
- Discipline
- **Speed**
- Quality

Innovation by Alliances

- **Alliance** perceived as important by all members
- **Trust** between partners
- **Clear** project planning
- **Defined** tasks and milestones
- Frequent and effective **communication**
- **Actual** contribution from all partners
- Benefits perceived as **equally** distributed

360s with Tuckers' Model

Stage	Strategy	Keys
Forming	Coordinating and setting vision	• Create **Trust** • **Purposefully picking** the team • Define a **vision** for the project
Storming	Creativity and Planning	• Develop a **common view** and **mental** model • **Calm** the and project environment • Brainstorm how the project will be **approached**
Norming	Coaching and Empowering	• Get **feedback** from project team and stakeholders • Create an **operational** team structure • Feedback from the project team and stakeholders • Provide opportunity for leadership and development
Performing	Support and Execution	• Allow for **flexibility** in team **roles** • Allow for the **transfer** of **leadership** • Manage **conflict** and project **failure** or **success** • **Achieve** objectives

Considerations for Innovative Teams/Projects

- A priori knowledge of the expected project outcomes/results.
- Technological challenge/risk.
- Number of organisations involved.
- Level of experience of the team, including the technical expertise of its members.
- Joint collaboration experience of the team.
- Geographical distribution of the team, considering physic and cultural differences.
- Adequate method for assessment of performance

Open Source and IP

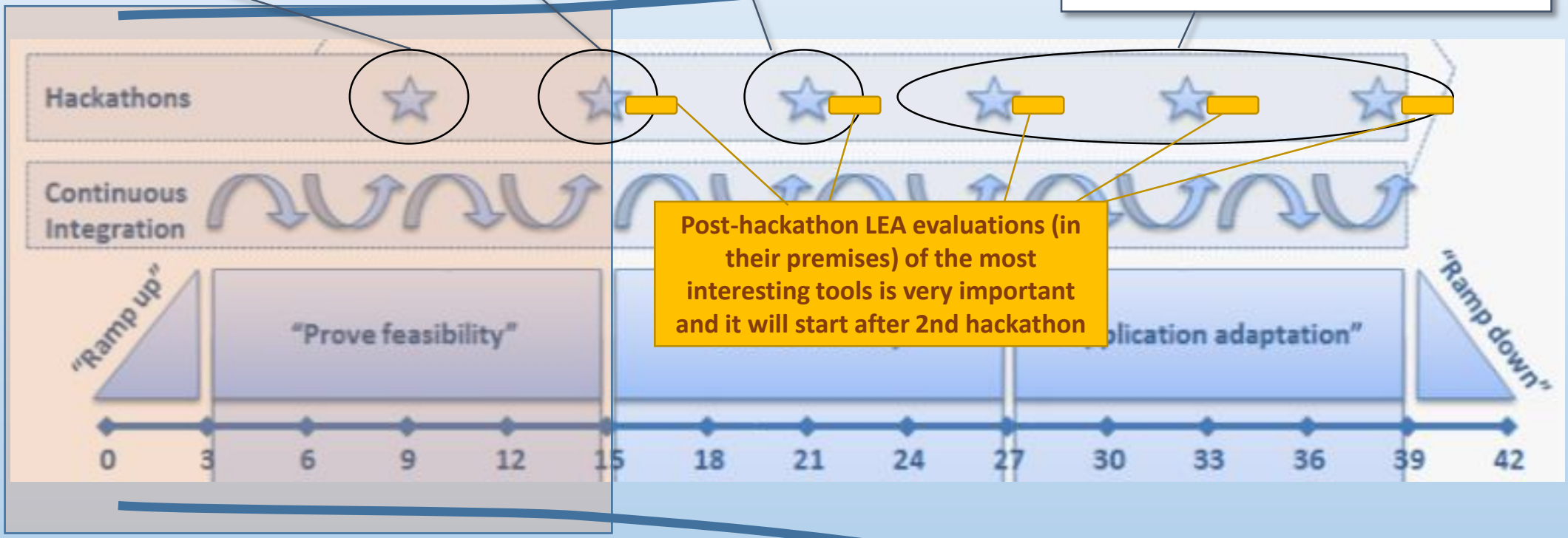
- Challenges:
  - Inadequacies of Consortium Agreement Models
  - Options in the H2020 AMGA
  - Internalisation of IPR Risk
  - Exploitation and Commercialisation Rights
  - Open in a Closed Community….
  - You can’t give something away for free if it’s not yours
- Models:
  - Complete or Partial License
  - **Transaction** Based Charges
  - **Mixed** Models
  - **User Types** Model
  - “**Give and Take**”
  - **Subscription** Model
  - **Pay** on **Deploy** Model
  - **Hybrid** Models
  - Open Source with **Ring-fencing**

Methodology and Inclusion

- BDUF (Big Design Up Front) methodologies they are suited to long and complex projects where the specification and goals are clear, and risk management is prioritised.
- Anamorphic or agile adaptive methods adapt to changing or loosely defined scope and require iterations in development.
- Hackathon derives from the words “hacking” and “marathon” in effect rapid and crude development
- ASGARD chose Hackathons as a methodology for many reasons:
  - To gauge readiness of the technologies,
  - Invite public(‘ish) opinion on the direction of ASGARD
  - Allow flexibility the research plan and goals
  - Means of multiplying the number of people testing and validating the technologies.
- For the LEA community this has been adapted in ASGARD

As the project makes progress it will open itself to additional stakeholders

- Focus on PROCESS; using background technologies
- Focus on INTEGRATION; “Low hanging” novel tools
- Focus on FINE TUNNING processes and integration; more novel solutions
- Focus on COMMUNITY BUILDING; MATURE processes and integration; more novel solutions
- Additional LEAs and stakeholders



Post-hackathon LEA evaluations (in their premises) of the most interesting tools is very important and it will start after 2nd hackathon

Conclusions

- Roles of project **brokers** and **principals** must be shared
- **Leadership** opportunities must be given
- **Trust** in cooperative innovation is easily undermined
- **Open Source is hard**
- **Governance** in **public** funded research and **agile** methods can mix
- **Hackathons** are an effective means of **Open Innovation** and **Validation** of Technologies
- Agile and creative research and innovation methods benefit from an **understanding** of **team dynamics**
- If the approach **scale** remains to be seen
- **Right methodology** for the right type of project (or the task in hand)
- After the 3rd hackathon (May'18), once there are sufficient number of new tools available and the processes put in place for the preparation and running of the hackathons are fine-tunned, additional LEAs and relevant stakeholders will be invited to participate (to join the ASGARD community!)