# Report: First EAB Workshop

| | | | |
|---|---|---|---|
| Name of meeting: | **EAB Workshop #1 Trento** | Date of Meeting: | **11/07/2017** |
| Minute Taker: | Garazi Juez. **Editors:** Huáscar Espinoza and Cristina Martinez | | |
| Attendees: | **Miren Illarramendi (EAB member)**<br>**Timo Varkoi (EAB member)**<br>**Johnny Marques (EAB member)**<br>**Marion Lepmets (EAB member)**<br>**Anders Sandin (EAB member)**<br>**Kurt Tschabusching (EAB member)**<br>**Laurent Fabre (EAB member)**<br>**Tim Kelly (EAB member)**<br>Huáscar Espinoza, Garazi Juez (TEC)<br>Stefano Puri (INT)<br>Thomas Gruber (AIT)<br>Barbara Gallina (MDH)<br>Jose Luis de la Vara (UC3)<br>Gaël Blondelle (ECL)<br>Ran Bi (RPT)<br>David Deharbe, Thierry Lecomte (CLS)<br>Alberto Debiasi (FBK)<br>Benito Caracuel (TLV) | | |
| Presentations: | Website: http://www.amass-ecsel.eu/content/external-advisory-board<br>For AMASS partners, located in SVN: SVN\AMASS_collab\04_Meetings_and_Workshops\2017_09_11-12_Trento_EAB-Workshop-1\Presentations | | |

## Agenda

**Monday, September 11 (FBK premises)**

| Start | End | Description | Speaker |
|---|---|---|---|
| 9:00 | 9:30 | Project Outline | Huáscar Espinoza |
| 9:30 | 10:00 | Technical Overview | Barbara Gallina |
| 10:00 | 10:30 | Selected Case Studies | Benito Caracuel, Helmut Martin and Thierry Lecomte |
| 10:30 | 11:00 | Coffee break | |
| 11:00 | 11:50 | Project Outreach and Community Building | Ran Bi and Gaël Blondelle |
| 11:50 | 12:20 | Intra and Cross-Domain Reuse | Barbara Gallina |
| 12:30 | 13:30 | Lunch | |
| 13:30 | 14:00 | Architecture-Driven Assurance | Stefano Puri |
| 14:00 | 14:30 | Multi-concern Assurance | Thomas Gruber |
| 14:30 | 15:00 | Seamless Interoperability | José de la Vara |
| 15.00 | 16:30 | EAB Feedback Brainstorming | Moderated by Huáscar Espinoza |
| 16.30 | 17:00 | Coffee break | |
| 17:00 | 17.30 | Wrap-up | Moderated by Huáscar Espinoza |

**Minutes**

Everybody introduced themselves. Presentations are available in the link indicated above. Some selected noted are collected below.

1. **Project Outline (Speaker: H. Espinoza)**
   - AMASS promotes a strong connection between architectural design and certification issues
   - AMASS looks for achieving a balance on safety and cybersecurity
   - AMASS develops a platform to harmonise the terminology of different domains by means of the AMASS Reference Architecture: including meta-models (how to harmonise the management of the assets).
   - AMASS also enhances the connections with other external tools
   - AMASS partners are involved at OMG (UC3 and TEC), in particular in the System Assurance task force.
   - First AMASS prototype is centered on the basic building blocks in terms of the baseline tools: Papyrus/CHESS, OpenCert and EPF Composer.
   - It is emphasized how important industrial impact and dissemination is.
   - Question from Laurent Fabre: are all the work packages on going? Answer: Yes, all the WPs are already running.
   - Question Laurent Fabre: more than one year has passed by since the project started. Are the results right now what you expected at the beginning of the project? Answer: Yes, it will be shown during the meeting in the different slots and videos..

2. **Technical Overview (Speaker: B. Gallina)**
   - Inconsistencies can happen when safety managers work with excels and words [Slide 4]
   - AMASS aims to systematise reuse by also exploiting concepts such as product lines and ontology-based technologies [Slide 6]
   - OSLC: AMASS is considering to use ontologies, which semantically relate the different pieces of information [Slide 11]
   - It is important to understand the interfaces between the different teams. Of course, the safety manager would still have to "use his/her intellectual work but some of the tasks would be automated [Slide 12].
   - Cross-domain case study is focused on COTS and DO-254 to the reuse of conformance with automotive standards into the avionics domain [Slide 13].
   - Feature diagram for product line engineering. To link pieces of information: process + product + assurance case [Slide 14]
   - Question Laurent Fabre: Have you developed any new tool for the first prototype? Answer: no new tools have been developed for the first prototype but some functionalities were added (documented in deliverables D3.4, D4.4, D5.4 and D6.4) and the baseline tools were integrated. In fact, it was not really easy to integrate the different tools from previous projects. In other words, the integration between the tools related to the first prototype and basic building blocks was quite complex: Papyrus/CHESS (system component specification), OpenCert (assurance, compliance) and EPF (compliance during the planning phase)

3. **Case Study CS1 (Speaker: B. Caracuel)**
   - Compliance of IEC 61508, IEC 62443, IEC 62351 industrial standards
   - Compliance gap analysis is really important for Schneider
   - Two assurance projects, which will be connected in future CS1 iterations: Safety RTU and Security RTU.
   - Question Tim Kelly: Have you already modelled IEC 62443 in OpenCert? Tim wanted to know if we have faced any issues when modelling, for instance, IEC 62443. Answer: We mentioned some difficulties we faced when trying to model IEC 62351, which is more product oriented. Important

also to remark that only some parts of the standards have been modelled.

- Question about standardisation and SACM. We will see in future AMASS prototype iterations how to align to the SACM standard, because a new version was recently released.
- Question: What are the benefits of doing it in this way (AMASS model-based approach) w.r.t. no model-based approaches? Answer: We have got two tasks in the project to evaluate that related to metrics and quantification. Benchmarking Framework in D1.3 (metrics definition) and Benchmarking realization itself in D1.7. The deliverable regarding the aforementioned metrics (D1.3) will be delivered by the end of September 2017.
- We will evaluate how much we can reduce in costs because of following this approach.
- Question from Timo: which are the AMASS tools supporting compliance management? Answer: baseline tools are EPF Composer (definition of the process -activities, artifacts, …-)**,** OpenCert: the meta-model collects information coming from the standards.
- The case studies provided feedback for the tools refinement.
- D1.4: report for the case studies. We have notified the EAB members that they can download the deliverable from the webpage, since it is public.

**4. <u>Case Study CS3 (Speaker: H. Helmut)</u>**

- Model Vehicle with different platforms. Failures can happen in the vehicles or communication.
- Model-based and contract-based development
- System modelling in CHESS and contract-refinement by means of OCRA
- Question Laurent Fabre: What does degradation cascades mean? Answer: The answer has been provided by specifying it as failure and graceful-degradation related.
- Question Tim Kelly: How does everything (architecture modelling and argumentation) fit together? Answer: We consider this is a good case study to evaluate that.
- Tim Kelly considers the approach quite specific and not generic anymore. Barbara answers highlighting how variability could solve that. Tim Kelly agrees but continues arguing how it is not generic anymore because the system needs to be modelled by Papyrus/CHESS. So to some extent, he thinks some requirements are imposed. Some aspects between the different approaches between OPENCOSS and SafeCer have been discussed (how in OPENCOSS they were not going inside the artifacts and in SafeCer yes because the architecture was modelled). Barbara explains that a conceptual meta-model exists and that CHESS represents and instance of it. Thus, given the presence of the conceptual meta-model, the genericity is guaranteed.

**5. <u>Case Study CS5 (Speaker: T. Lecomte)</u>**

- Platform Screen Door case study for SIL 3.
- Papyrus: system functions**.** Code generation assessment
- Question Laurent Fabre: But… what does Papyrus for security mean? What´s the feedback regarding Sophia tool? Answer. Sophia tool has been explained. Good experience on using Papyrus for security (Thierry).
- Huáscar emphasized the importance of reuse also to achieve issues concerning certification between different countries (reuse).
- Timo has made a comment: “the global approach is a bit complex. Is your approach for big companies? Or is it for medium/small companies?” Good feedback in terms that AMASS approach can be applied also to SME (Clearsy is a SME).

**6. <u>Dissemination, Exploitation, Training, Standardization (Speaker: R. Bi)</u>**

- Question Laurent Fabre: what do you consider training? Answer: Internally, explanation between how tools such as EPF, Papyrus/CHESS or OpenCert work. Externally, explain how the different tools work to external industrial partners. For instance, Barbara has given a course in Sweden regarding certification by means of an e-learning platform.

- Question Tim Kelly: how are you involved in standardization? Answer: Thomas Grüber answered. How, for instance, AIT is involved in working groups: IEC 62443, railway VDE security (in Germany) and so on. Thomas has highlighted multi-concern aspects of AMASS as a key issue.
- Question Tim Kelly: Are you trying to give feedback to certification people about how the modelling should be done? Give them inputs regarding methods to be included in the standards? Answer Thomas: yes, we are trying to promote some techniques and giving inputs regarding safety and security issues (e.g. how IT security is not sufficient in such systems).
- Tim Kelly remarked how it is not easy at all to be involved and to influence certification groups. Thomas answered by saying how important it is at least to be involved in such groups and how we try to influence to the extent that we can in terms of, for instance, developing safety-security co-engineering methods.
- Huáscar mentioned that we are aware of those difficulties and we are open to recommendations about how we could better influence them.
- Ran Bi explained how we could contribute by applying open source solutions as well.
- Tim Kelly found out an issue on some timeline [slide 10].

### 7. <u>Community Building and Industrial Outreach (Speaker: G. Blondelle)</u>

- Community Building has been presented and connections to other projects explained
- We have asked the EAB to give us feedback regarding possible connected/related projects which have not been considered.
- We have explained how it is possible to create and contribute to an Open Source Community through Eclipse/Polarsys.
- Huáscar highlighted how we would like to get feedback regarding impact and open source approach.
- Question Tim Kelly: what are really the success facts? If we do not get the tools to be used, that would be an issue. Answer: Gael responded saying that the fact of storing the code on Github is not a solution. We are aware that it is difficult that by the end of the project we can have industrial adopters of the tools, however, if industry starts using these approaches, slowly will be a big success. We want to be ready when this (like the use of models for certification) happens.
- Huáscar mentioned how we are offering some innovative results: mature for the basic functionalities and prototypes for others. We understand it is not an easy task; however, we will put a lot of effort on several activities such as external training to industry. We are aware that the main feedback should come from industry.
- Question: Antonio: What about the qualification of the tools? Answer: Huáscar answered by saying that tools do not really require qualification for now but we are studying the needs for this in WP5.

### 8. <u>Intra and Cross-Domain Reuse (Speaker: B. Gallina)</u>

- Cross-intra domain reuse and compliance management topics addressed.
- AMASS addresses the semi-automatic generation of certification artifacts. Reuse possibility via ontologies and variability management based on product lines best practices. AMASS does not intend to build upon individual solutions for each dimension (process/product/assurance case) but proposes to adopt an orthogonal solution.
- Explanations concerning how EPF Composer supports process modeling.
- Tim does not think that it is possible to model a certain standard in only one way (different interpretations of the same standard). How to calculate the reducible amount of effort on certification. Difficult to measure. Enough mentioning it. Barbara replied that this is why a product line-based approach can be helpful. Different interpretations could be collected as variants (allowed variants), whenever certification went through successfully.
- Difficulties on understanding why within the AMASS approach different solutions such as CACM and EPF/BVR can be found. "Difficulties on understanding the big picture". Activity and artefact concepts are related within the CACM. And now you have got EPF Composer/BVR as well. I am

including activities which were not considered. Does this mean that concepts of variable activities are in two different places? For instance, criticality level seems to be modelled in two different places to me. Is there an overlap of concepts? Why to do it in this way?

- Barbara and Huáscar answered by saying there could be some overlaps on certain concepts between CACM and external tools, but this will be managed by bridges and transformations between models.
- Barbara remarked how in OPENCOSS project, product and argumentation variability could not be modelled.
- AMASS Demo Video has been played.

**9. Architecture-Driven Assurance (Speaker: S. Puri)**

- Claim the system is sufficiently safe. Associate a contract to a system component**.** The assurance case reflects how the system has been designed.
- Question Tim Kelly: what does contract associated to the assurance mean? Answer: a contract is related to a claim.
- Question: how is the semantic behind that relation/link/transformation? Suggestion from Tim: review the system-component meta-model and we should pay attention when defining the semantics for the transformation between the system component and the assurance case.
- S. Puri reminds that in the last review we had the input regarding defining system boundaries ' "defining system boundaries is a difficult task (open systems, open environment…)"

**10. Multi-Concern Assurance (Speaker: T. Gruber)**

- Question Tim: How to do the trade-off method? How to resolve the conflicting requirements? A bit of skepticism on hot to perform a quantitative analysis on security. Furthermore, Tim Kelly informed as about the trade-off argument approach. We have answered by saying that we were aware of that and we considered that in D4.1. Furthermore, he has emphasized that it is not only a trade-off between safety and security but we should consider more the following issues when deciding which is the best o most appropriate architecture:
- The best architecture will depend on the standard to apply**.** The best architecture will depend on the project costs**.** The best architecture will depend on the criticality level.
- It has been mentioned that we are also working on this areas (design trade-offs) in terms of WP3. Outcome: design trade-off really important!
- Question: more discussions ongoing about how to use contracts and what the difference to a claim is. Tim explained assurance case contracts. The main goal is to connect two assurance cases to check if they can match together. "Agreement glue between two assurance cases = assurance case bindings".
- Question Tim: are we going to update the argumentation editor? Yes, also to make it compliant to the standards.

**11. Seamless Interoperability (Speaker: J. de la Vara)**

- We need to provide interoperability means that can be used by any tools.
- The possibility of generating connectors for any tool is ongoing.
- Automatic transformation between artifacts.
- Connection between artifacts: this functionality should be extended.
- How to exploit information on traceability based on OCRA: the different EAB members didn´t quite understand the need of OCRA.
- Traceability with CAPRA: Question Tim: Do all the models not have traceability to artifacts? Which is the universal model of traceability? Answer: Yes, the link is modelled. Maybe the link of the meta-model is not enough for what we would need to relate. For instance, indirect dependencies to allow reuse.

- Question Tim: why not to add the information we would need directly in the meta-model? Otherwise, we have got the risk that people can create links "on-the-fly". There should be some reasoning on what information can be related to what by means of a meta-model.
- Different discussions have taken place on why to have different tools doing the same thing. Then, we have explained how we have got many external tools. However, we should better define which tools are going to be external and which ones part of the AMASS platform.

**BRAINSTORMING SESSION**

Mind maps of the brainstorming at shown at the end of this document.

**A. AMASS Challenges**

**Architecture-Driven Assurance (Contract-Based Approach)**

- Link design assumptions or contracts to the assurance case information. The meta-model should be reviewed (Tim). The system component meta-model has been presented and analyzed.
- Tim: methodologically is difficult to comprehend what a design contract is. Review the semantics between contract and argumentation.
- Jose Luis has remarked that anyway we need to take into account that maybe someone does not want to develop the argumentation.
- In brief: work more on the semantics: system/component/design ' argumentation
- Tim´s remarks:
  - Assurance cases are just about behaviours, the assurance of the component of course depends on the behaviour,
  - design by contracts: then how the modular assurance is aligned (clarify)
  - Connection of formal languages for contracts can be an issue (formal specification of contracts)
  - SACM goes behind anything that exists nowadays.
  - Review IEC 15026
- Stefano Puri: yes, the semantics of the links need further work and we need to better clarify certain issues; it will become more clear when we will provide information about argument fragments generation approach.
- Question: which are the benefits w.r.t. RECOMP? RECOMP only works on compliance checks with Standards. TEC uses RECOMP results for OPENCOSS and AMASS.

**Multi-concern Assurance (Safety and security co-assurance)**

- Question Tim: is security aware safety only our goal?
- Question Lauren Fabre: Are the authorities demanding a security case alone? Answer: Tim: we have got a UK defence project asking for a separated security case on its own. (It is a project requirement, not a standard)
- Tim: safety cases were stable, with automated driving not anymore.
- Tim: Adding monitors in different places ' autonomous systems.
- Thomas: Approach to safety and security is different. Security process should adapt to safety.
- Tim: we will really need to understand each other and align.
- Laurent Fabre: the approach looks promising but many things you have mentioned are not really possible in real life.

**Interoperability and Tool Support**

- Tool Qualification: we are aware regarding the difficulties on providing reliable tools.
- Assurance of our tools was not planed and we have not currently the effort to do so.
- Huge number of tools/Amount of tools to make everything work together, too ambitious.

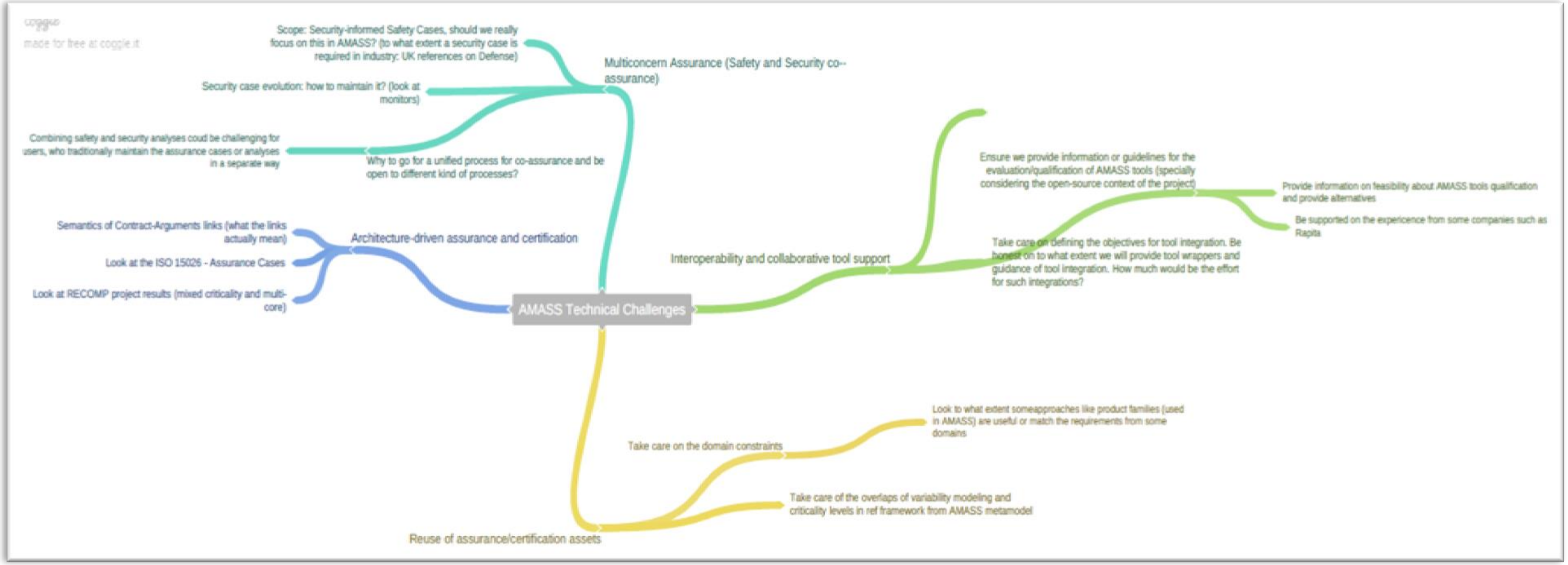
- Tim: I have the impression that it only works in the context of certain configuration of the tools. You really need to document how to do the wrapper or to connect tools together. "To document everything is scary"
- We are already working on how to connect everything on Semantics Level. For instance, Sabotage with Papyrus/CHESS or model-based safety analysis tools.
- Tim: there are a lot of set-up costs. If you want to take people cost realistically you need to model that set up costs in a good way. How consuming or how much effort does it have to model the standards? Like it happened in OPENCOS…
- Take into account the effort on configuration (standard modelling and so on)
- General comment (not only here): clearly state which tools are going to be implemented and which ones are part of AMASS building blocks. Make clear which tools are going to be used in which case study: CASE STUDIES and WPs and TOOLs require better relationship (moved to AMASS industrial impact).
- Laurent Fabre: issues regarding Open Source and Qualification need to be considered and better explained.
- Huáscar: evaluate the approach of the qualification of the assurance case editor in comparison with other alternatives like performing a manual review.
- Lauren Fabre has suggested that we should take into account what is feasible and what is not. Tim has suggested that maybe Rapita can offer support on tool qualification.

**<u>Reuse of assurance/certification issues</u>**

- How to deal with specific needs from different domains? This approach can be more useful in some domains compared to others.
- We have modelled some generic taxonomy (SEooC, IMA…)
- Tim suggested changing the problem into product families. According to Tim, "everything" goes in the direction to solutions such as AUTOSAR even if this does not make the problem easier.
- The problem of component integration is really relevant.
- Process families: requirements of standards. Specific process model of a standard. Take care of this when meta-modelling not to model the things twice.

**<u>B. AMASS Industrial Impact</u>**

- Timo: Acronyms. It would be nice for people who are not familiar with the terminology to explain those terms: INDUSTRIAL TERMINOLOGY ADOPTION. (Take care of the language).
- Marion Lepmets: Why AMASS tools are better compared to other possible solutions? A global view with respect how, for instance, WP3 tools could help to the state of the art/practice or w.r.t. the assurance tools they use could help. → Include user stories.
- How to influence the standardisation bodies need to be better addressed. → Tim suggested on giving them feedback regarding difficulties when modelling for instance the security standard mentioned before (IEC 62351).



AMASS Technical Challenges

Multiconcern Assurance (Safety and Security co--assurance)

Scope: Security-informed Safety Cases, should we really focus on this in AMASS? (to what extent a security case is required in industry: UK references on Defense)

Security case evolution: how to maintain it? (look at monitors)

Why to go for a unified process for co-assurance and be open to different kind of processes?

Combining safety and security analyses coud be challenging for users, who traditionally maintain the assurance cases or analyses in a separate way

Architecture-driven assurance and certification

Semantics of Contract-Arguments links (what the links actually mean)

Look at the ISO 15026 - Assurance Cases

Look at RECOMP project results (mixed criticality and multi-core)

Interoperability and collaborative tool support

Ensure we provide information or guidelines for the evaluation/qualification of AMASS tools (specially considering the open-source context of the project)

Provide information on feasibility about AMASS tools qualification and provide alternatives

Be supported on the experience from some companies such as Rapita

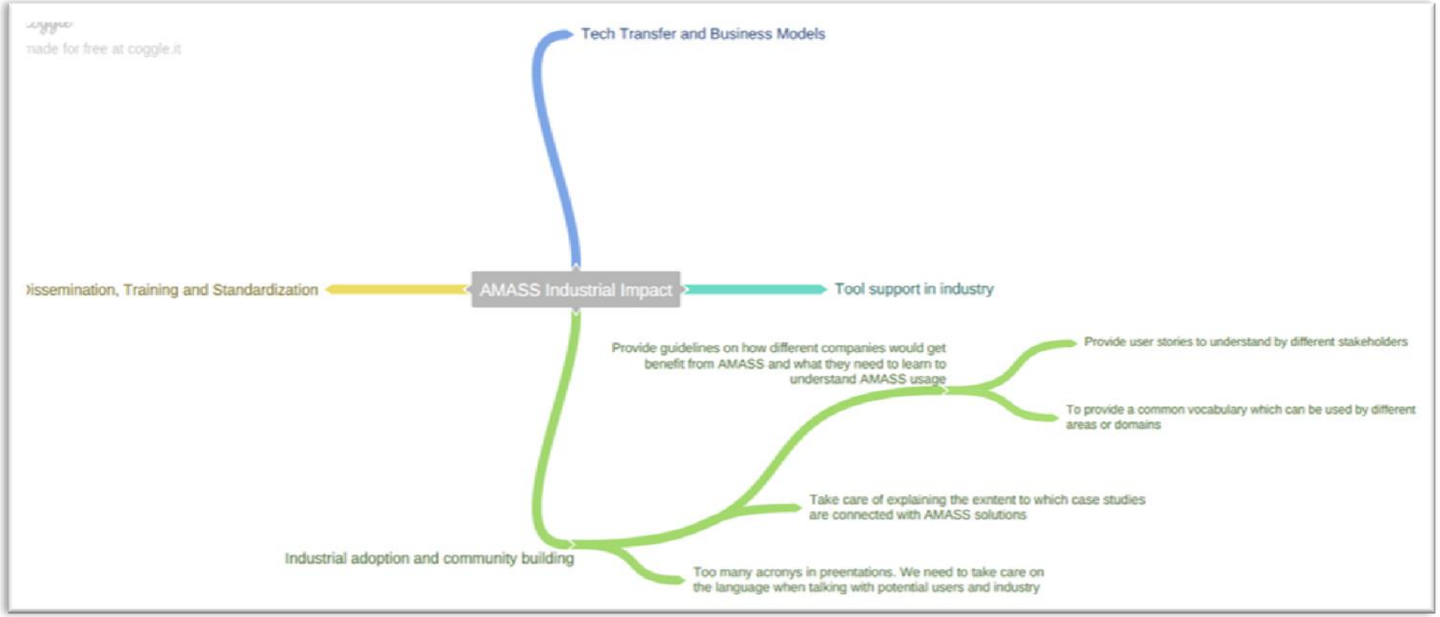
Take care on defining the objectives for tool integration. Be honest on to what extent we will provide tool wrappers and guidance of tool integration. How much would be the effort for such integrations?

Reuse of assurance/certification assets

Take care on the domain constraints

Look to what extent someapproaches like product families (used in AMASS) are useful or match the requirements from some domains

Take care of the overlaps of variability modeling and criticality levels in ref framework from AMASS metamodel



AMASS Industrial Impact

Tech Transfer and Business Models

Tool support in industry

Dissemination, Training and Standardization

Industrial adoption and community building

Provide guidelines on how different companies would get benefit from AMASS and what they need to learn to understand AMASS usage

Provide user stories to understand by different stakeholders

To provide a common vocabulary which can be used by different areas or domains

Take care of explaining the exntent to which case studies are connected with AMASS solutions

Too many acronys in preentations. We need to take care on the language when talking with potential users and industry