# Systematic review on STPA
# Final Results

**Carlos H. N. Lahoz**
Aeroastro Dept MIT
Instituto de Aeronautica e Espaco IAE
**Synara R. G. Medeiros**
Phd Candidate
Instituto Tecnologico da Aeronautica ITA

# Acknowledgements:



Instituto de Aeronautica e Espaco (IAE)


Aeroastro-MIT

System Engineering Research Lab

Research sponsored by:


2015/2016 Post-doc fellowship


supplementary grant 2015


Remarks:

*This Systematic Review don't have the ambition to cover 100% of the STAMP/STPA research works found over the internet and digital libraries, but aims to collect the most expressive works of STAMP/STPA*

# SR on STPA: outline

- Context and Motivation
- Systematic Review (SR)
- SR on STPA
- Discussion

# SR on STPA: context

São José dos Campos is a important industrial and research center in Latin America: with one big and aprox.130 medium&small aerospace enterprises

Institute of Aeronautics and Space IAE
National Institute of Space Research INPE
Tecnological Institute of Aeronautics ITA
Embraer SA
Avibras, Orbital, Compsis, Equatorial, Omnisys,...

BOEING

2012: Research and Technology Center installed in S J Campos

SAAB

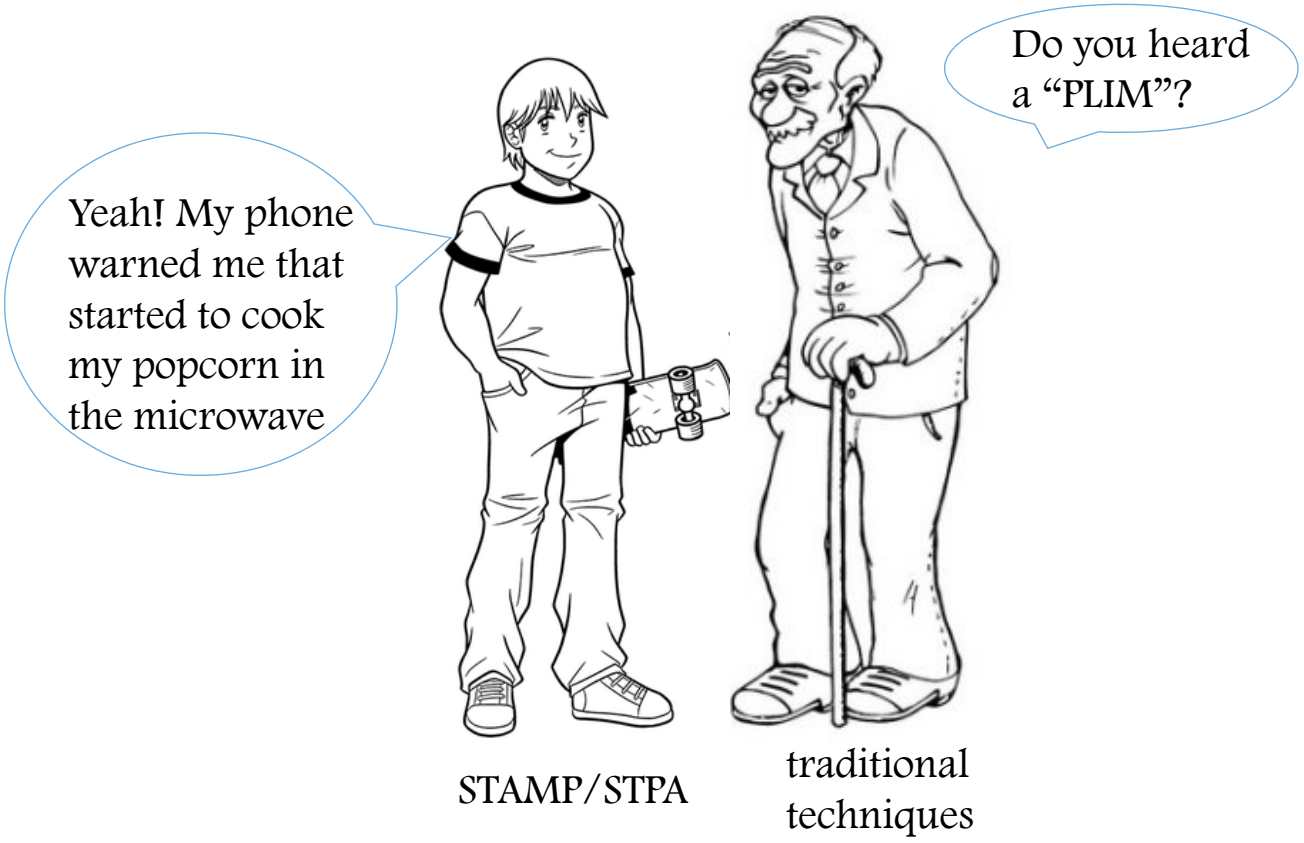
2014: Signed the contract to construct and deliver the 36 Gripen aircraft to the Brazilian Air Force ($5.4 billion). It includes comprehensive industrial co-operation between the countries in areas such as research and development and transfer of technology which will be performed over approximately ten years (involving Embraer, IAE, ITA and others players)

# Motivation

- To understand how the STAMP/STPA users are performing their analysis
- To identify lessons learned from users
- Synthesize evidence, identify research trends, open problems, improvement opportunities and new directions for future investigations
- Finish the Systematic Review that started in 2015 (STAMP Workshop) when the preliminary results were presented

# Motivation

- Although the traditional techniques have played an important role in system safety, it's time to open space for new approaches to understand and deal with the dynamics and complexity of modern systems

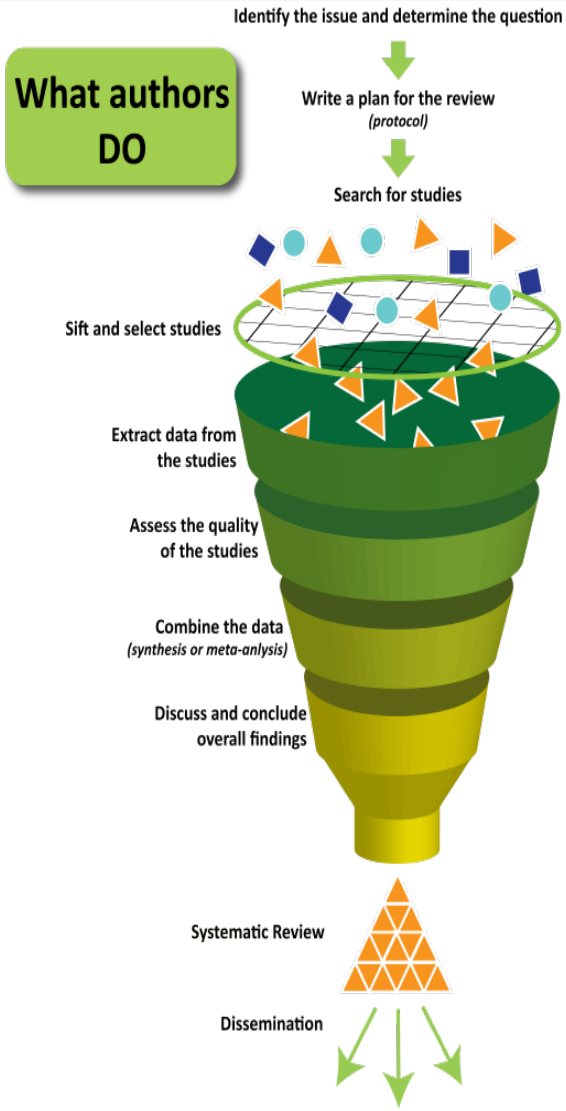


# Systematic Review: definition

- The purpose of a systematic review is to sum up the best available research on a specific question. This is done by synthesizing the results of several studies. The Campbell Collaboration. www.campbellcollaboration.org/what_is_a_systematic_review. Access: March, 21 2016

- The development of a systematic review aims to establish a more formal and controlled process of conducting this type of investigation, avoiding the introduction of the biases of the unsystematic review (literature reviews in general). Pitangueira, Maciel, Barros. Software Requirements Selection and Prioritization Using SBSE Approaches: A Systematic Review and Mapping of the Literature, Journal of Systems and Software, Elsevier, In Press, October 2014

# Systematic Review: processes




**1 – PLANNING**

~Identification of the need for a review

~Development of a review protocol

**2 – CONDUCTING**

~Selection of primary studies

~Data extraction & synthesis

**3 – REPORTING**

~Reporting the review

Source: Centre for Health Communication and Participation La Trobe University, Australasian Cochrane Centre

# SR on STPA: planning

-Identification of the Needs & a Review Protocol

- Provide a summary of the research about STPA
- Looking for evidences about the works (level of maturity of the works )
- Acquire relevant information to guide new development projects
- Find new directions for future investigations

# SR on STPA: conduction

Research Question

- Research Questions (1/2):

*(for all works in SR)*

RQ.1: What is the AREA where the STPA was applied?

RQ.2: What KIND of work is ? (STPA application, method, tool or approach?)

RQ.3: Does the work is discussing the STPA with TRADITIONAL hazard analysis?

RQ.4: What is the level of EVIDENCE of the study (practical results)?

# SR on STPA: conduction

Research Question

- Research Questions (2/2):

(JOURNALS, CONFERENCES, THESIS, BOOKS CHAPTERS, etc)

**RQ.5A**: Does the work is clearly presented (RIGOR of the research)?

*Capacity to describe the STPA and the study case; if the analysis is repeatable and the impact of the results*

(WORKSHOPS)

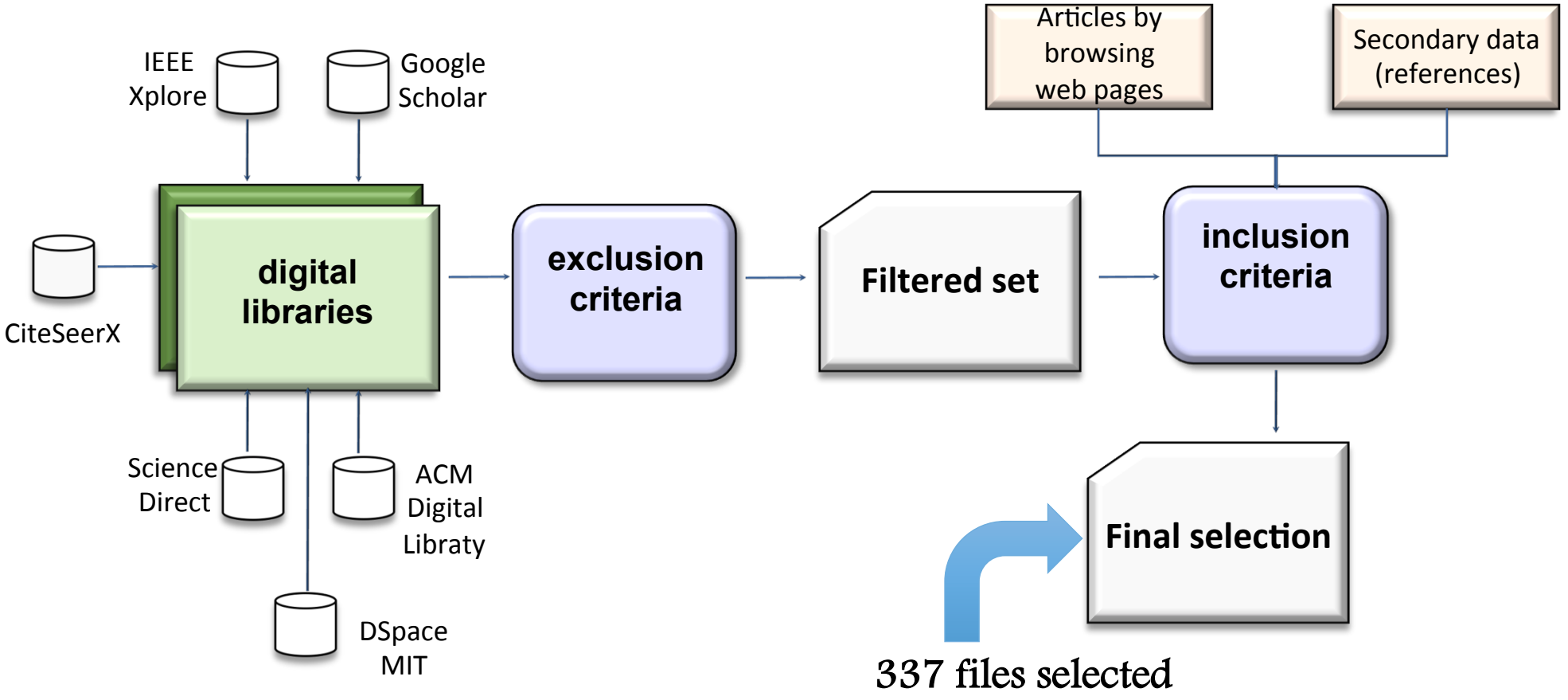
**RQ.5B**: Does the goals of the presentation were achieved ?

*objectives+ research/application+conclusion*

# SR on STPA : conduction

Search Strategy

~ Searching for the studies (1/3)



# SR on STPA: conduction

Search Strategy

~ Searching for the studies (2/3)

- Digital Libraries: IEEE Xplore, ACM Digital Lib, CiteSeerX, Google Scholar and ScienceDirect, DSpace@MIT) using the target search string (STAMP and/or STPA and/or CAST

WEB OF SCIENCE™

ACM DL DIGITAL LIBRARY

Google Scholar

ScienceDirect

MIT Libraries DSpace@MIT

CiteSeerx 6M

CAPES

- Search Strategy: to minimize the risk of missing relevant papers, we too included additional papers manually via:

✓ Personal web pages, references found in papers already in the pool (secondary references), specific venues (STAMP Workshops, ...)

# SR on STPA: planning

-Data extraction

Exclusion Criteria

- Exclusion Criteria: Works whose content does not discusses any aspect related to "STAMP", "STPA" or "CAST" (even the work dealing with safety, but not related to STAMP / STPA)

Inclusion Criteria

- Inclusion Criteria: other works found in universities or web sites that discuss or describe characteristics of "STAMP", "STPA" or "CAST", including case studies and experience reports

# SR on STPA: conducting

Book[B](and Chapters) = 5
Conference[C]=20
Symposium[S] = 5
Doc thesis[D]= 16
MsC dissertation[M] = 49
Journal[J]=53
Paper[P]= 10
Poster[O] = 3

Report[R] = 13
Tutorial[T] = 13
Workshop[W] = 150

# SR on STPA: conducting

Book[B](and Chapters) = 5
Conference[C]=20
Symposium[S] = 5
Doc thesis[D]= 16
MsC dissertation[M] = 49
Journal[J]=53
Paper[P]= 10
Poster[O] = 3

Report[R] = 13
Tutorial[T] = 13
Workshop[W] = 150

Chapters and book:

-Safety-Critical Systems: Problems, Process and Practice, 2009

-Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems, 2009

-Engineering a Safer World, 2011

-Influencing the Quality, Risk and Safety Movement in Healthcare: In Conversation with International Leaders, 2015

-Advances in Aviation Psychology, 2014

# SR on STPA: conducting

Book[B](and Chapters) = 5
Conference[C]=20
Symposium[S] = 5
Doc thesis[D]= 16
MsC dissertation[M] = 49
Journal[J]=53
Paper[P]= 10
Poster[O] = 3

Report[R] = 13
Tutorial[T] = 13
Workshop[W] = 150

Doctorate thesis
14 MIT
01 Missouri Univ Scien&Tech
01 Paris Institute of Technology

# SR on STPA: conducting

Book[B](and Chapters) = 5
Conference[C]=20
Symposium[S] = 5
Doc thesis[D]= 16
MsC dissertation[M] = 49
Journal[J]=53
Paper[P]= 10
Poster[O] = 3

Report[R] = 13
Tutorial[T] = 13
Workshop[W] = 150

Master Science dissertations:
42 MIT
01Heriot-Watt University, Scotland
01 MacMaster Univ, Canada
02 Norwegian Univ Scienc&Tech
02 Lund University, Sweden
02 ITA, Brazil

# SR on STPA: conducting

Book[B](and Chapters) = 5
Conference[C]=20
Symposium[S] = 5
Doc thesis[D]= 16
MsC dissertation[M] = 49
Journal[J]=53
Paper[P]= 10
Poster[O] = 3

Report[R] = 13
Tutorial[T] = 13
Workshop[W] = 150

(*) IF=Impact Factor: average number of citation received in the journal per year(s)

Journals:
-Communications of the ACM (IF=3.511)
-American Institute of Chemical Engineers Journal (IF=2.748)
-Reliability Engineering & System Safety (IF=2.41)
-Ergonomics (IF=2.023)
-Safety Science (IF=1.831)
-The Journal of the Human Factors and - Ergonomics Society (IF=1.694)
-Accident Analysis and Prevention (IF=1.647)
-IEEE Transactions on Dependable and Secure Computing (IF=1.35)
-Chinese Journal of Aeronautics (IF=1.07)
-Journal of Healthcare Engineering (IF=0.754)
-Journal of Energy and Power Engineering (IF=0.596)
-Journal of Spacecraft and Rockets (IF=0.533)

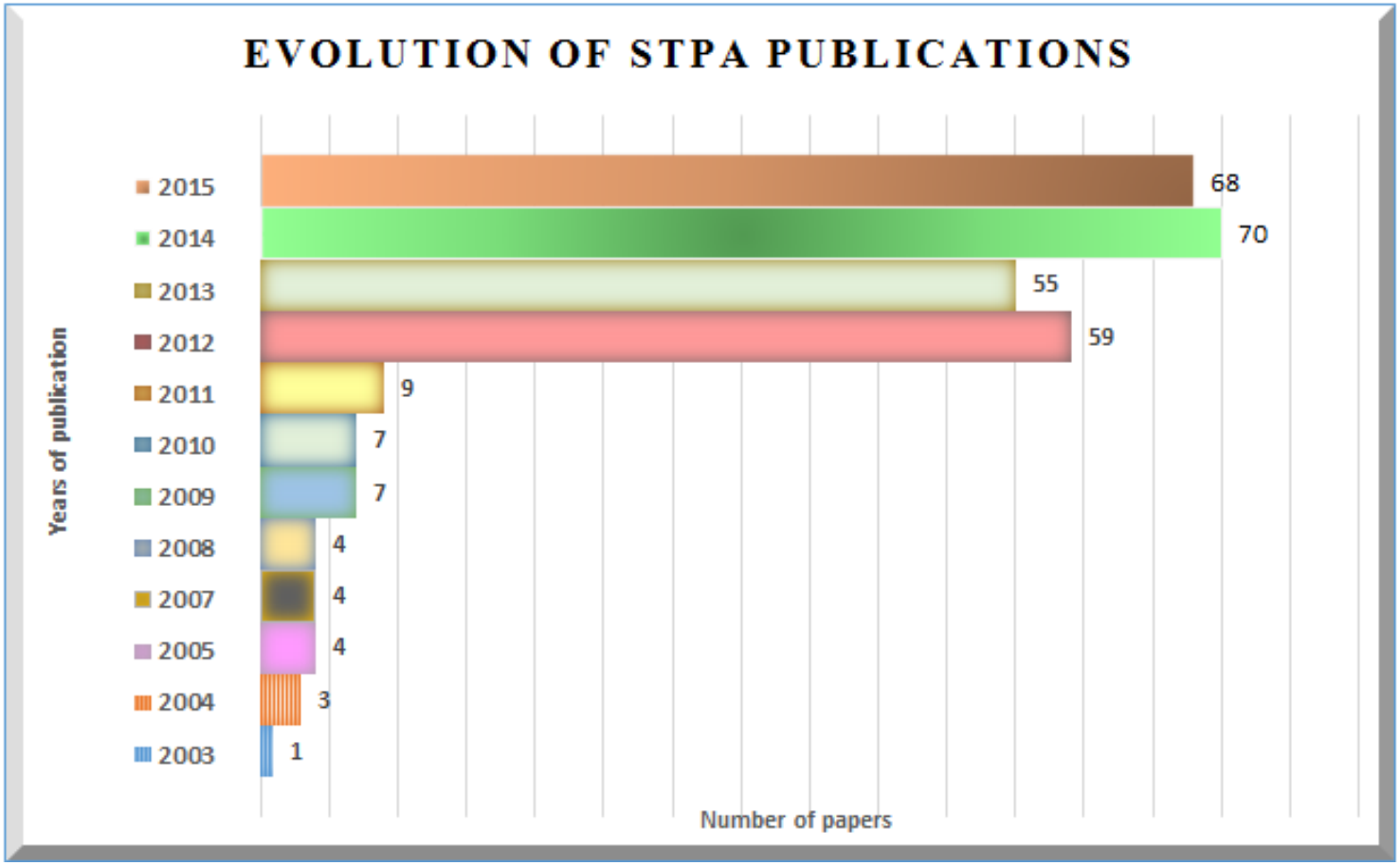
# SR on STPA: conducting

Book[B](and Chapters) = 5
Conference[C]=20
Symposium[S] = 5
Doc thesis[D]= 16
MsC dissertation[M] = 49
Journal[J]=53
Paper[P]= 10
Poster[O] = 3

Report[R] = 13
Tutorial[T] = 13
Workshop[W] = 150

Workshops:
01 Workshop on Investigation and Report of Incidents and Accidents 2003
01 NASA IV&V Workshop
26 STAMP Workshop 2012
32 STAMP Workshop 2013
28 STAMP Workshop 2014
11 European STAMP Workshop 2014
01 Workshop on New Security Paradigms
31 STAMP Workshop 2015
19 European STAMP Workshop 2015

# SR on STPA: reporting: publications




*It can be observed that since the mid –2000's had already published work on STPA. But it was in 2011 that the research on the subject grew in a sustancial form (book 2)*

(*) this picture is not including the total of the SR files

# SR on STPA: reporting

- Countries with STAMP/STPA works

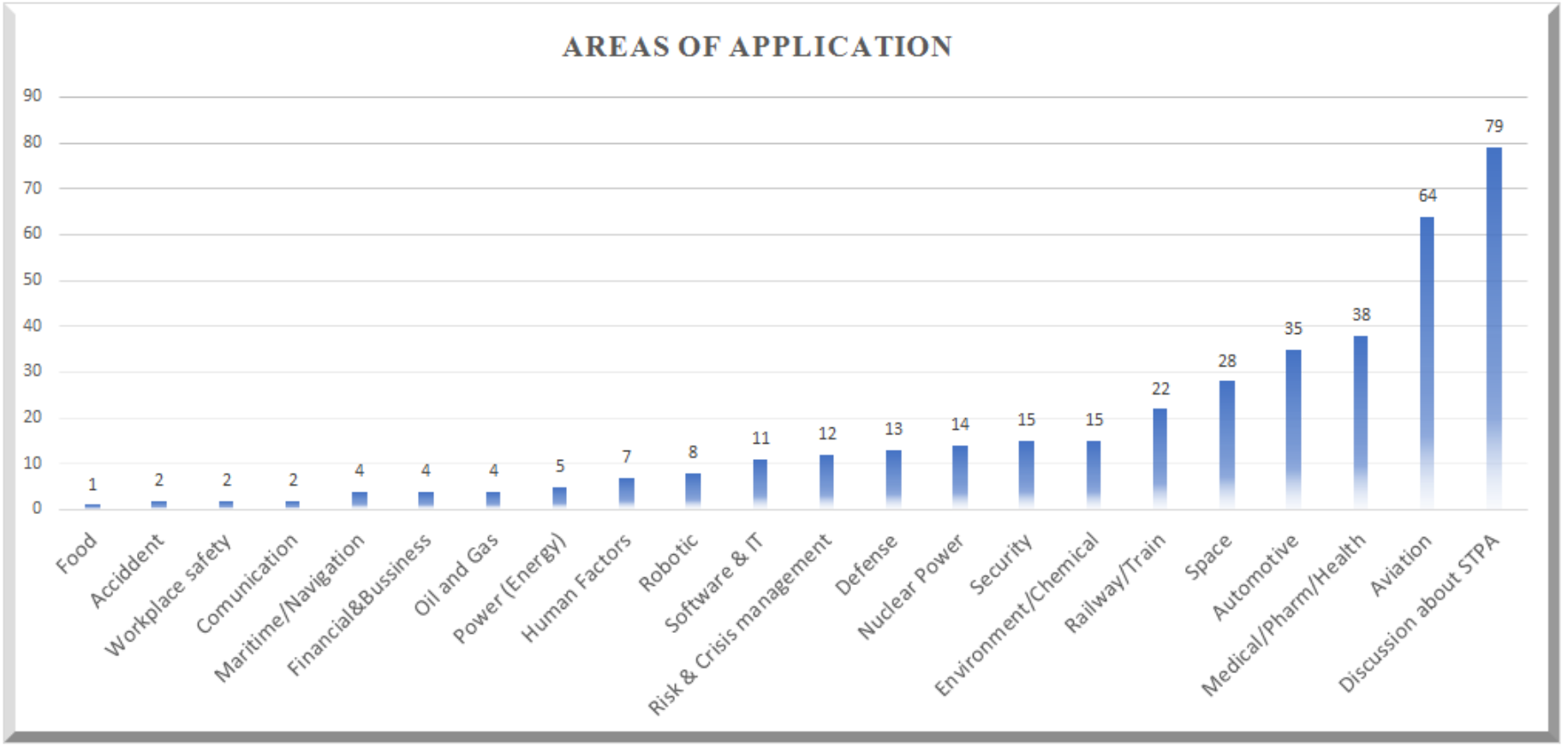
- Americas: Brazil, Canada, United States
- Europe: Estonia, England, France, Finland, Iceland, Ireland, Germany, Greece, Ireland, Norway, Spain, Sweden, Switzerland, The Netherlands
- Asia: China, Japan, Korea, India
- Australia

OBS: in 2016 : Austria, Brazil, China, England, France, Greece, Germany, Italy, Israel, Japan, Norway, The Netherlands, USA

Total of 26 countries

# SR on STPA: reporting

❑ SYNTHESIS 1: Areas of STAMP/STPA application

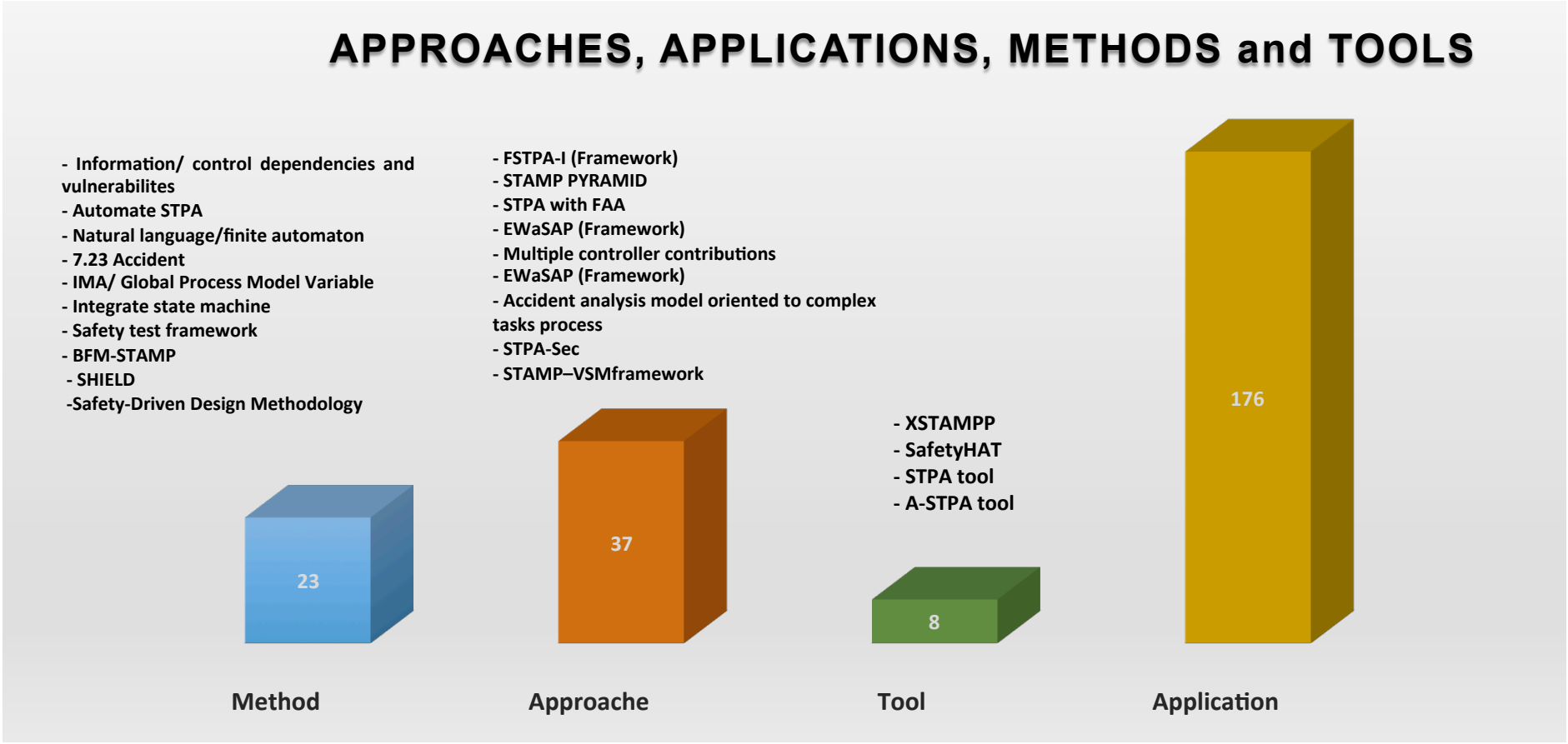



*Four main areas: aviation, medical, automotive and space.*
*Railway is another prominent area with 22 works.*
*New areas growing: environment, security and risk&crisis management*

(*) this picture is not including the total of the SR files

# SR on STPA: reporting

- SYNTHESIS 2: Kind of work (1/2)




(*) this picture is not including the total of the SR files

# SR on STPA: reporting

- SYNTHESIS 2: Kind of work (2/2)

The highlight for tools is the A-STPA and XSTAMP (Univ Stuttgart) follow by SafetyHAT and STPA/MIT

STPA Sec is a preeminent approach, with more than 12 works related

Techniques: we can highlight some complementary methods applied together with STAMP/STPA: Natural language into finite automaton, state machine, safety test, SHIELD (System Hazard Indication & Extraction Learning Diagnosis, Safety Requirement Generation Method, Safety-Driven Design Methodology, formalization model, among others

# SR on STPA: reporting

- SYNTHESIS 3: STPA and traditional hazard analysis techniques (1/3)

Project Risk Analysis = 4
FTA and FME(C)A = 20
HAZOP = 3
Safety cases =1
Assurance cases = 1

More recently, many works are starting to discuss STAMP/STPA with Leading indicators for risk (3 works) and risk analysis and management (5 works)

# SR on STPA: reporting

- SYNTHESIS 3: STPA and traditional hazard analysis techniques (2/3)

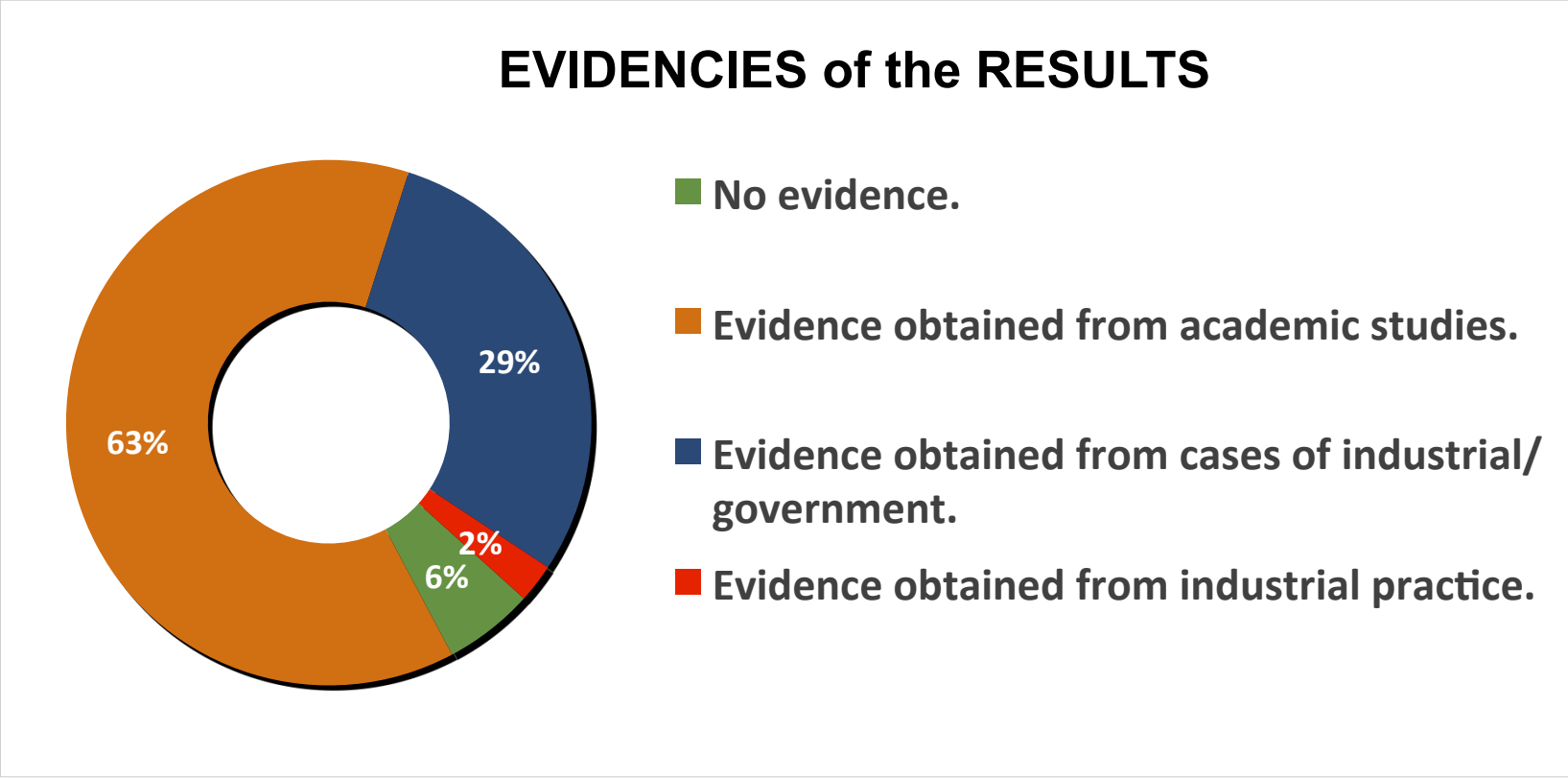
"…one study has performed an in-depth gap analysis between a STAMP and FMEA, found that when analyzing a system the STAMP were identified more hazards (175 vs 75)" Balgos, Y., A systems theoretic application to design for the safety of medical diagnostic devices, Master Dissertation, MIT 2012

"STPA provides a framework that allows for effective assessment and monitoring of producibility (quality, product compliance, cost, and schedule) risk indicators" Ball, A., Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development, Master dissertation, MIT 2015

"Whereas STAMP includes how the different control loops are affecting each other and may discover hazard that the HAZOP analysis does not catch" Hoel, F., Modeling Blowouts During Drilling Using STAMP and STPA. Master dissertation, Norwegian Univ Science and Technology 2012

# SR on STPA: reporting

❑SYNTHESIS 4: Evidence: maturity level of the results (case study)




One of the central issue in this SRs is identify the level of confidence in the conclusions and recommendations arising from the study case: the boundary between academic purpose and "industrial" purpose

(*) this picture is not including the total of the SR files

# SR on STPA: reporting

- SYNTHESIS 5A: study is focused, coherent and appropriately developed (case study or lessons learned?) 0=no; 0.5=partly; 1=yes

| | | |
|---|---|---|
| **RQ5.1** | Is the paper based on research (or is it merely a "lessons learned" report based on expert opinion)? | **Reporting** |
| **RQ5.2** | Is there an adequate description of the context in which the research was carried out? | |
| **RQ5.3** | Was the data collected in a way that addressed the research issue? | **Rigor** |
| **RQ5.4** | Was the data analysis sufficiently rigorous? | |
| **RQ5.5** | Does the researcher have experience in the case study area? | **Credibility** |

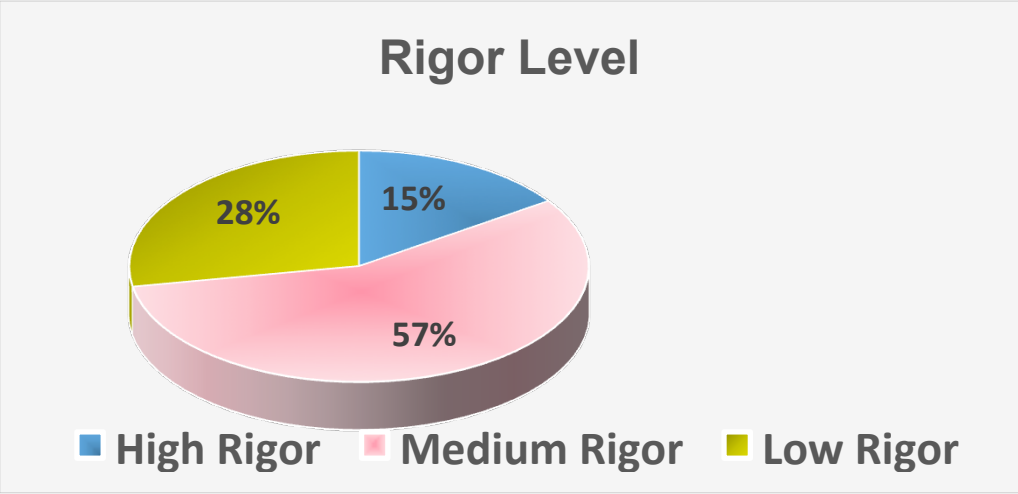
If neither answer equal zero:

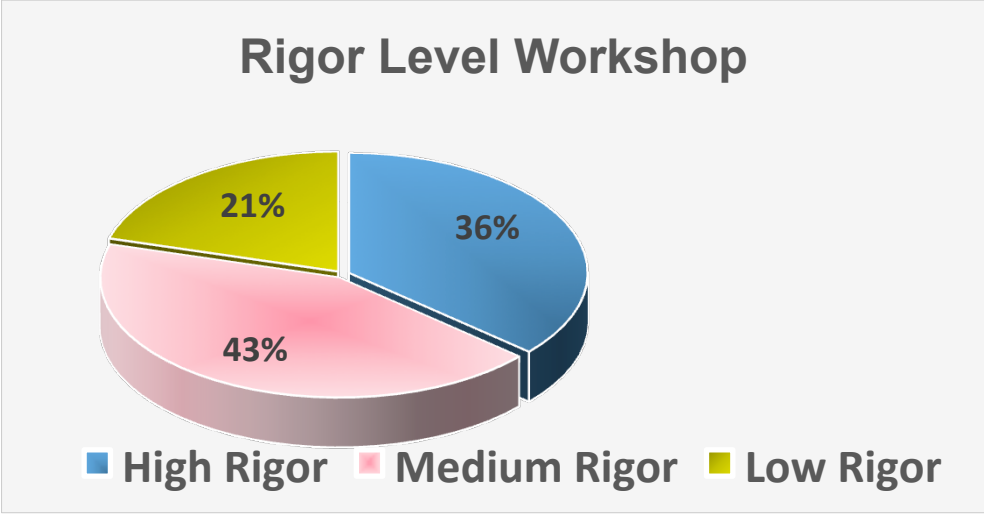
3.0:High rigor / 3.0 ≤ x ≤ 2.5: Medium rigor/ < 2.5: Low rigor

If at least issue equal zero: ≥ 3.5: Medium rigor / ≤ 3.0 Low rigor

# SR on STPA: reporting

- SYNTHESIS 5A: study is focused, coherent and appropriately developed (case study or lessons learned?)



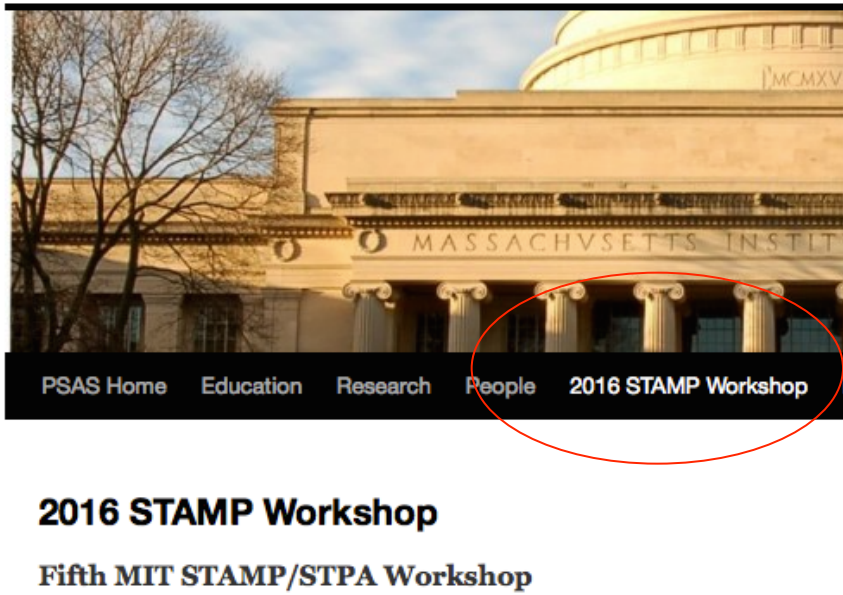




- SYNTHESIS 5B: The goals of the presentation (workshop) were achieved (for instance, objectives-research/application-conclusion)?

# SR on STPA : reporting

-Report the results

Presentations in the fourth and fifth STAMP Workshop(2015 & 2016)




Journal submission (just after the workshop-May/2016), including the Workshop 2016 presentations and more (recent) papers

Disseminate the results (and the list of references) in the "cloud"

Create a guide with the best practices (in Portuguese) to apply STAMP/STPA

# Discussion

- "STAMP/STPA can be analyzed not only safety aspects, but also functional goals" Thomas, J. Extending and Automating STPA for Requirements Generation and Analysis. STAMP/STPA Workshop 2012.

- "Besides to address misbehaviors due to software problems, may help address regulatory concerns" Torok, Geddes. Systems Theoretic Process Analysis (STPA) Applied to a Nuclear Power Plant Control System. STAMP/STPA Workshop 2013.

- "Identify potential hazard causes in human controller by analyzing patterns of mistakes caused by cognitive behaviors errors" Hoshino, N. Applying Human Mental Model to STAMP/STPA. STAMP Workshop 2014

# Discussion

- "Defining control structures: A critical part of STPA is the definition of the control structure during step 1, i.e. to define all relevant system components and their relationships" Asplund. Safety-Guided Design through System-Theoretic Process Analysis, Benefits and Difficulties. 30th International System Safety Conference, 2012

- "How to filter relevant contexts to hazards to avoid unnecessary scenarios?" Fleming C. ARP 4761 and STPA. STAMP Workshop 2014

- "STPA seems to be the most thorough method but it also needs the most time. Yet, for safety-critical systems, a high recall (number of safety requirements found) and coverage (types of safety requirements found) is probably more important" Abdulkhaleq, A. and Wagner, S. A Controlled Experiment for the Empirical Evaluation of Safety Analysis Techniques for Safety-Critical Software, EASE, 2015

# Discussion: (potential) future directions

- Deal with (and push to) the change of paradigm at conservative environments ~(safety) cultural changes in industry, government and organizations in general

- Approaches/Strategies to exchange the traditional safety/hazard/risk analysis to STAMP/STPA, mainly in regulatory environments (aeronautics and automobile)

- More research focus in how to work with multiple controllers (need more investment)

# Discussion: (potential) future directions

- How to choose (and define) the most critical scenarios? (the improvement started, but is a lot to do)

- Leading indicators applying to operational/improvement safety process (closing the safety loop)

- Improve the guide of how to apply the steps of the STPA - new Primer version - despite of the improvements already made, there are still many questions and expectations in STAMP workshops about this topic

# Systematic review on STPA:
# Final Results

Please, contact us to take part of this Systematic Research:

carloslahoz@gmail.com
synararosa@gmail.com