

Systematic review on STPA

A preliminary study

Carlos H. N. Lahoz

Instituto de Aeronautica e Espaco IAE

Synara R. G. Medeiros

EMBRAER





SR on STPA: outline

- ☐ Motivation
- ☐ Systematic Review (SR)
- ☐ SR on STPA
- ☐ Discussion
- ☐ References



Motivation

- ❑ To understand how the Systems – Theoretic Process Analysis (STPA) users are performing their analysis.
- ❑ To identify lessons learned of STPA users.
- ❑ Synthesize evidence, identify research trends, open problems, improvement opportunities and new directions for future investigations.

Systematic Review: definition

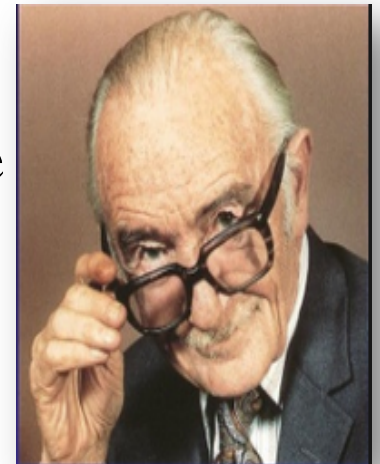
- ❑ A systematic review (SR) is a technique to identify, evaluate and interpret relevant research in an area of interest, a research question or a specific phenomenon of interest. [1]
- ❑ The goal of performing an SR is to follow a research process, methodically rigorous, in order to help to identify, analyze and interpret the available evidence related on a topic, of a particular subject, in a manner not biased and repeatable. [2, 3]
- ❑ “Evidence-based medicine”: Initially, SR was applied to medicine and health. Archie Cochrane's “ (1972) urged health practitioners to practice evidence based medicine.



Systematic Review: history

- ❑ 1962 – FDA requires drugs to show evidence of effectiveness
- ❑ 1972 – Archie Cochrane calls for use of evidence in medical decision making
- ❑ 1985 – 1990 – Book of systematic reviews on perinatal health topics
- ❑ 1992 – Cochrane Centre (UK) funded
- ❑ 2009 – PRISMA Standards for publishing SR
- ❑ 2013 – RAMESES standards for publishing meta-narrative

Archie Cochrane
(1909-1988)



Systematic Review: today

SR has been widely used to provide a concise summary of a given area of interest.

The screenshot displays a search interface with the following elements:

- Top Navigation:** Includes links for "Nova Busca", "Convidado(a)", "Meu Espaço", "Minha conta", and "Identificar".
- Search Bar:** Contains the text "systematic review" and a "Buscar" button.
- Results Summary:** A red box highlights the text "Resultados de 1 - 10 para 407.235 para Portal de Periodicos".
- Database Logos:** Logos for ".periodicos.", "CAPES", and "ScienceDirect" are visible.
- Search Filters:** A section titled "Refine filters" includes a "Year" filter with a dropdown menu.
- Search Results:** A red box highlights the text "Search results: 744,658 results found for (Systematic review)".
- Search Options:** Includes a "Purchase" button and an "Export" button.
- Search Results List:** A list of search results is shown, with the first result titled "Using metrics in Agile and Lean Software Development - A systematic literature review".
- Web of Science Overlay:** A semi-transparent overlay on the right side shows the "WEB OF SCIENCE™" logo and search results. A red box highlights the text "Resultados: 57.564 (de Todas as bases de dados)". Below this, it says "Você pesquisou por: Título: ('systematic review') ...Mais".

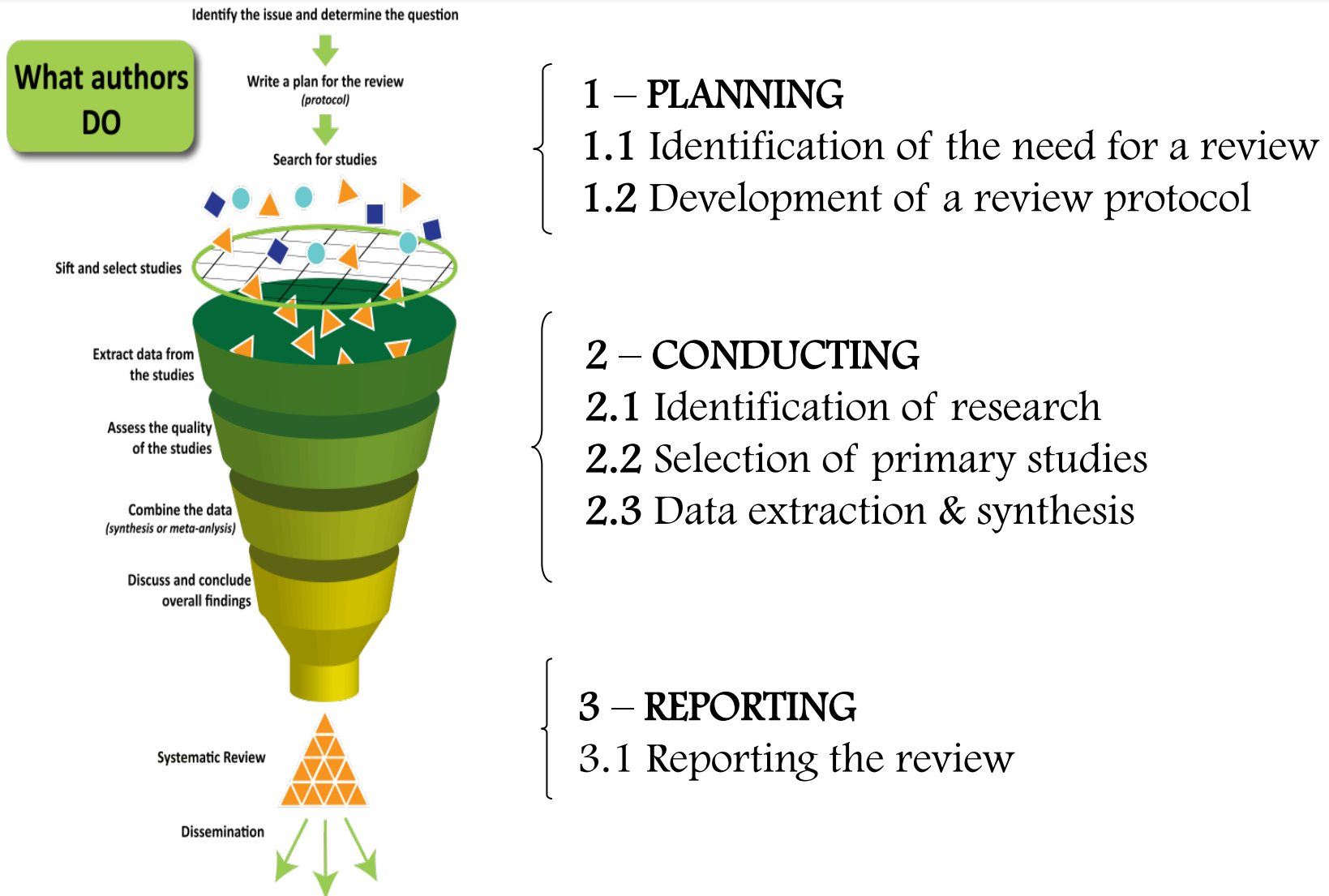
Systematic Review: ethic

Fundamental ethical principles in SR [4]:

- ☐ Research based on the results of experimental studies
- ☐ Protection of persons
- ☐ Qualification of investigators
- ☐ Positive benefit/risk assessment
- ☐ Avoid publication bias



Systematic Review: processes



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



SR on STPA: planning

1.1 IDENTIFICATION OF THE NEED FOR A REVIEW

Provide summary of STPA research evidence that could be found relevant to help to guide development projects and to indicates new directions for future investigations.

SR on STPA: planning

1.2 DEVELOPMENT OF A REVIEW PROTOCOL

- ❑ The review protocol specifies the methods used to carry out the SR.
- ❑ Defining the review protocol prior to conducting the SR can reduce research bias.



SR on STPA: planning

Research
Question

1.2 DEVELOPMENT OF A REVIEW PROTOCOL

- ❑ Formulate the research question: the critical issue in any SR is to ask the right question and easier to undertake a review when the question is specific and limited in scope.

Q.1: What are the areas where the STPA is being applied?

Q.2: What are the approaches and tools being applied along with the STPA?

Q.3: What works discuss the STPA and traditional hazard analysis techniques?

Q.4: What is the level of evidence of the case – studies?

Q.5: What are the limitations of the current STAMP/STPA research works?

SR on STPA: planning


Search
Strategy

1.2 DEVELOPMENT OF A REVIEW PROTOCOL

- ❑ To identify the search terms using Boolean expression 'OR' and combining main search terms using 'AND' in Digital Libraries.
- ❑ The following general search terms were used for identification of primary studies:

Review AND (Systematic OR Literature)
AND (STAMP OR STPA OR CAST)
AND (System OR Theoretic OR Process Analysis).

SR on STPA: planning



Search
Strategy

1.2 DEVELOPMENT OF A REVIEW PROTOCOL

- ❑ The search was made on Digital Libraries (IEEE Xplore, ACM Digital Lib, CiteSeerX, Google Scholar and ScienceDirect) using the target search string.
- ❑ 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 refs.).
 - ✓ Specific venues (Workshop STPA).

SR on STPA: planning

1.2 DEVELOPMENT OF A REVIEW PROTOCOL



Exclusion
Criteria



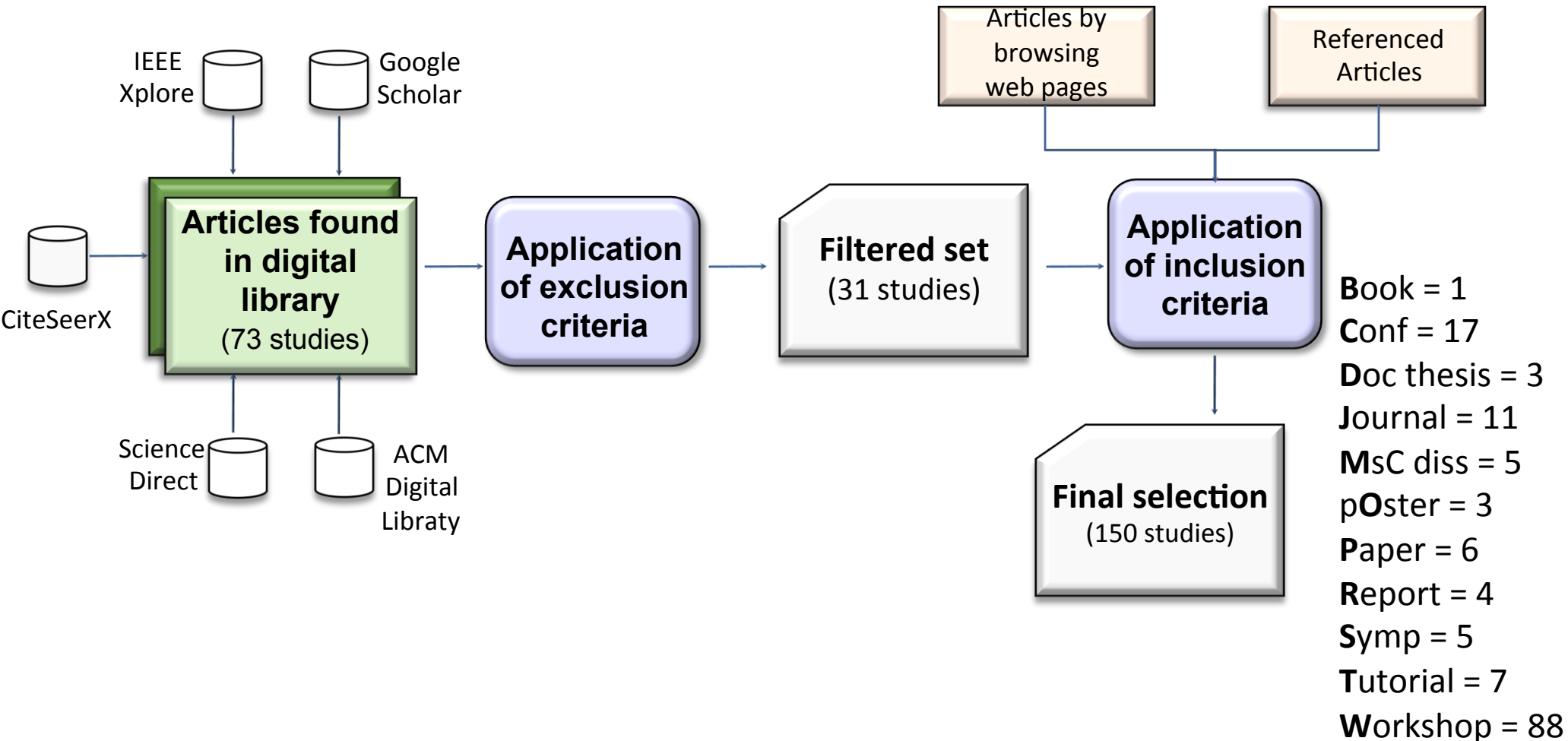
Inclusion
Criteria

- ☐ Exclusion Criteria: Article has no content that explicitly discusses any aspect related to "STAMP", "STPA" or "CAST".
- ☐ Inclusion Criteria: Papers in universities or web sites that analyze or describe characteristics of "STAMP", "STPA" or "CAST", including case studies and experience reports.

SR on STPA : conducting

2.1 SELECTION OF PRIMARY STUDIES

2.2 IDENTIFICATION OF RESEARCH





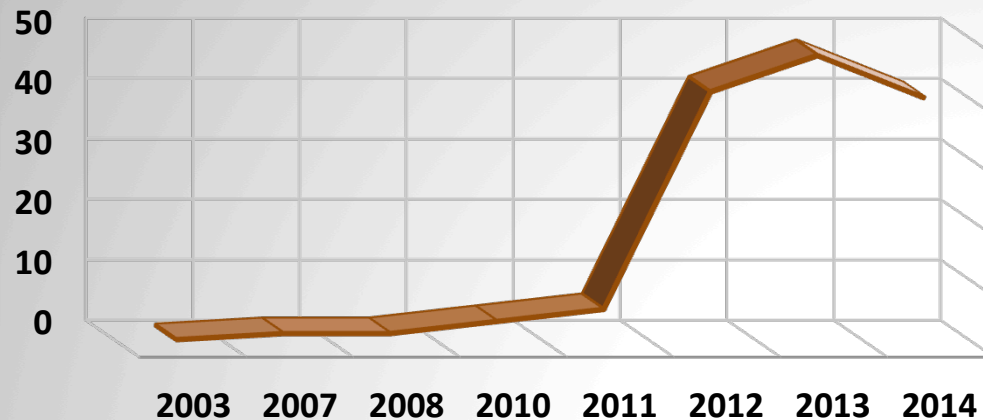
SR on STPA : conducting

2.3 DATA EXTRACTION AND SYNTHESIS

- ❑ Extracted information about the studies (population, intervention and outcomes) was tabulated in a manner consistent with the review question.
- ❑ A spreadsheet was created to compile the 150 works identified in this Phase 1 (data extraction).
- ❑ The results (synthesis) were compiled in tables and graphs that will allow the inclusion and exclusion (bias) of new work, part of Phase 2 of this SR.

SR on STPA : conducting

Evolution



It can be observed that since the mid-2000's had already published work on STPA.

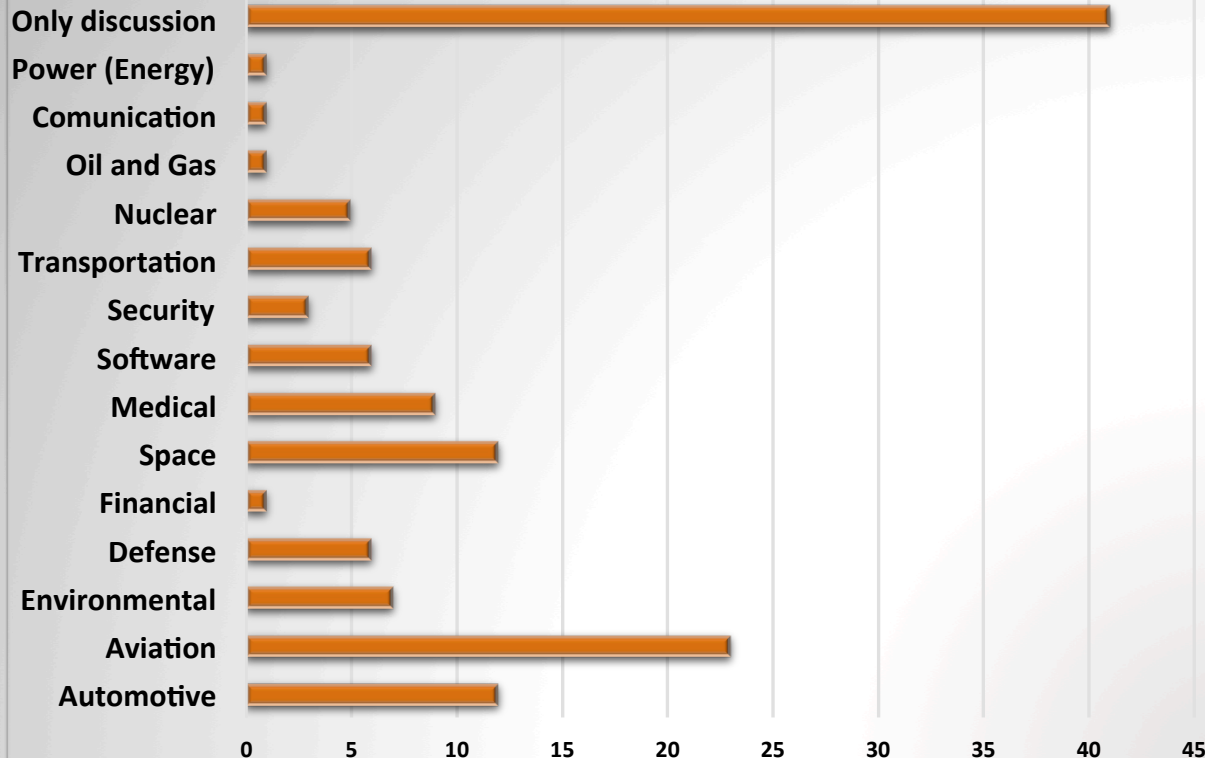
But it was in 2011 that the research on the subject grew sustancial form.

SR on STPA : conducting

RESULTS: TYPES OF PROBLEMS THE STPA HANDLE

❑ SYNTHESIS 1: Areas of STAMP/STPA application

Areas of Application



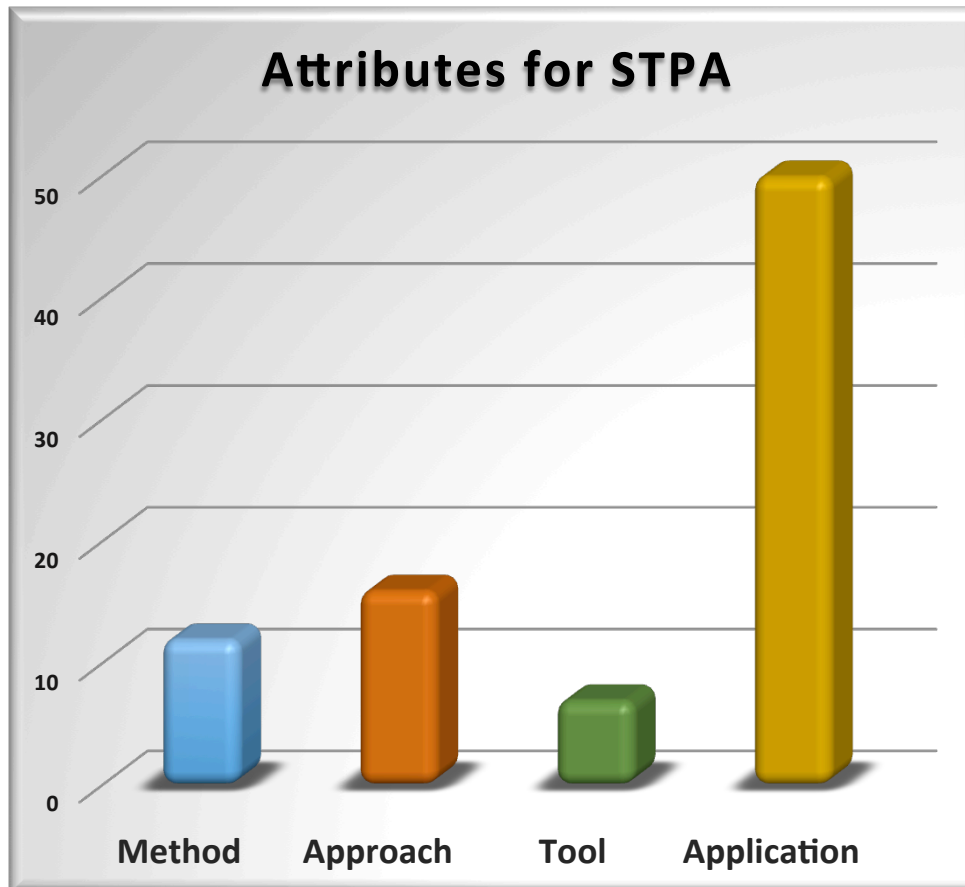
*The **aviation** (and the space, two focus of Aeroastro Department) is that have more studies in recent years.*

***Transportation** (train, mostly) was another prominent area with more than ten works.*

SR on STPA : conducting

RESULTS: TYPES OF PROBLEMS THE STPA HANDLE

❑ SYNTHESIS 2: Approaches, methods and tools applied along with STPA



The highlight for tools is the A-STPA that has 5 works (will still be applied the bias).

...and, of course the STPA tool from MIT-Aeroastro! And SafetyHAT

Despite the STAMP / STPA be relatively new and the most of the works are applied directly with the technique, we can highlight some complementary methods applied together: state machine, safety test, formalization model, etc.

SR on STPA : conducting

❑SYNTHESIS 3: STPA with traditional hazard analysis techniques

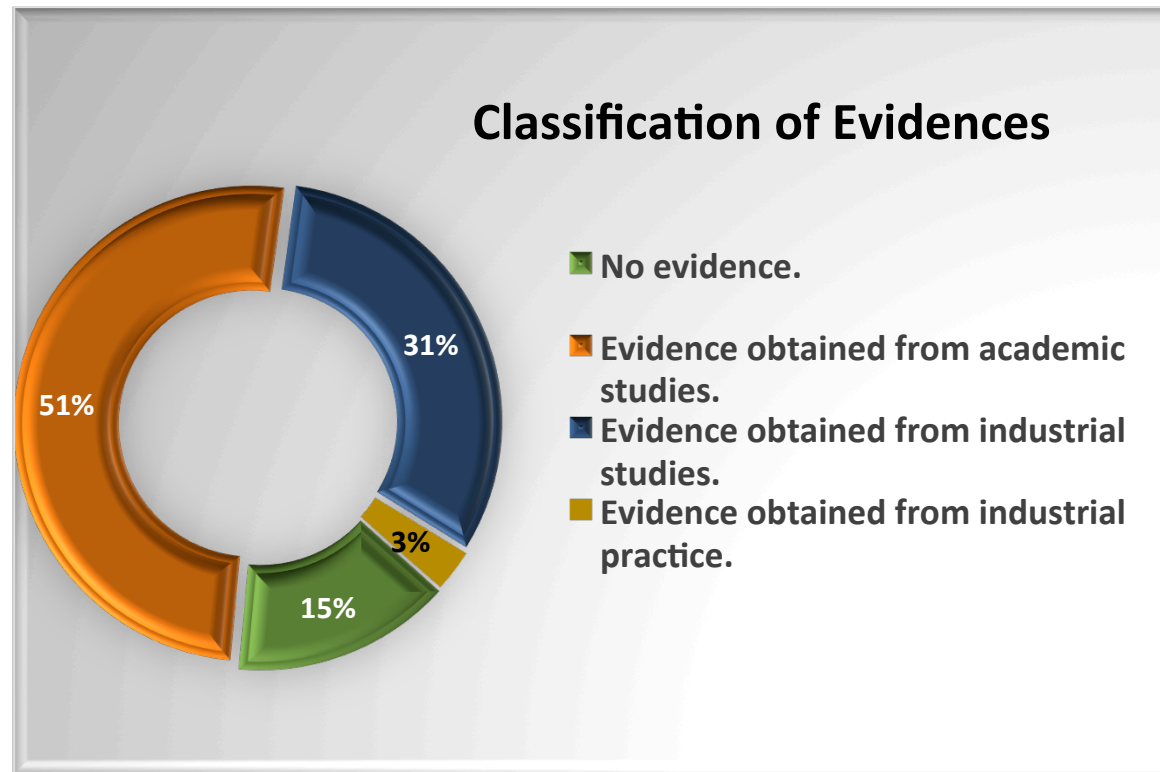
Of the 150 articles found, only 13 (10%) discuss the STPA and traditional hazard analysis techniques.

FMEA	HAZOP	FTA	Risk Management
5	1	3	4

It is not clear if the STPA is a complementary or substitutive technique (to be identified in the next phase of the SR). This discussion is still little explored: Important subject for future research

SR on STPA : conducting

□SYNTHESIS 4: Case study – level of evidence



One of the central issue in SRs is how much confidence we can place in the conclusions and recommendations arising from studies and experiences.

Classification of evidences STAMP/STPA: theoretical applications (academic) and practical applications (industry).

SR on STPA : conducting

□SYNTHESIS 5: Case study – level of evidence

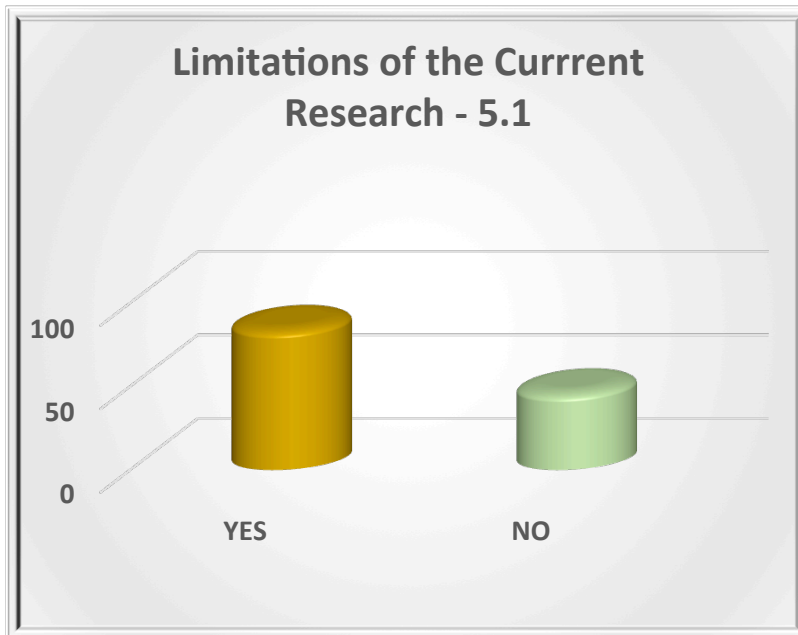
Questions:

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

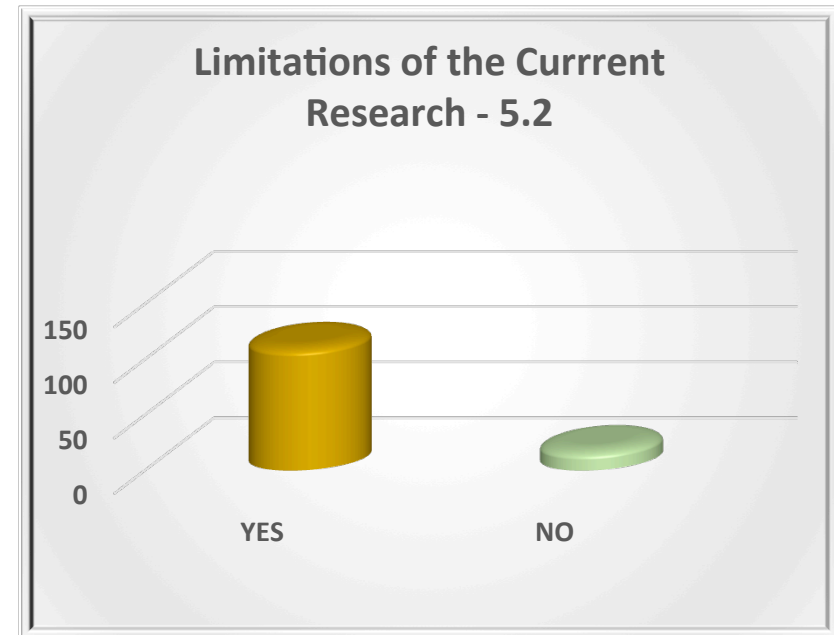
SR on STPA : conducting

❑ SYNTHESIS 5: Case study – level of evidence

It is important to emphasize that were included in Phase 1 many presentations from STAMP Workshops (approximately 58%) who did not have the same publishing rigor like a journal paper, report or thesis



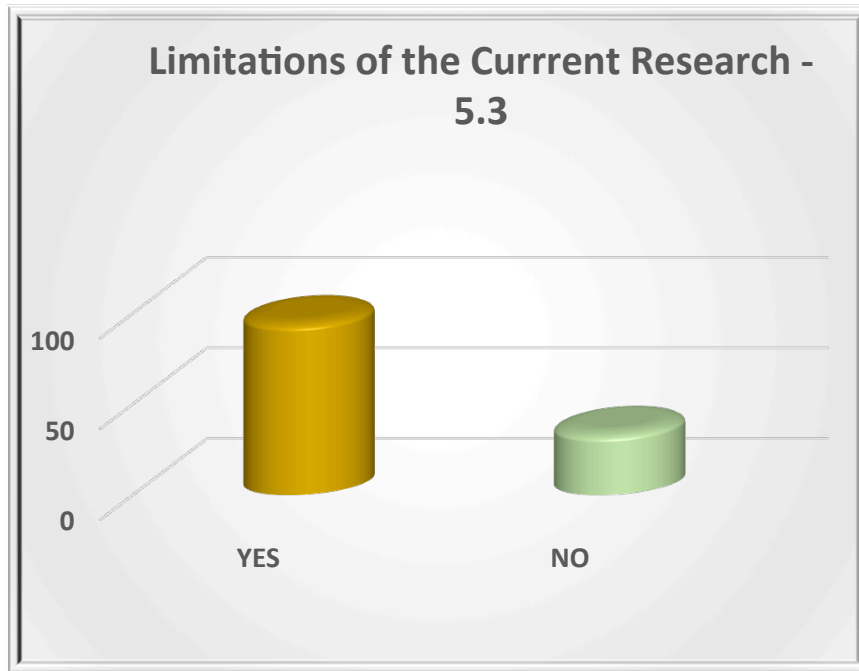
Is the paper based on research (or is it merely a “lessons learned” report based on expert opinion)?



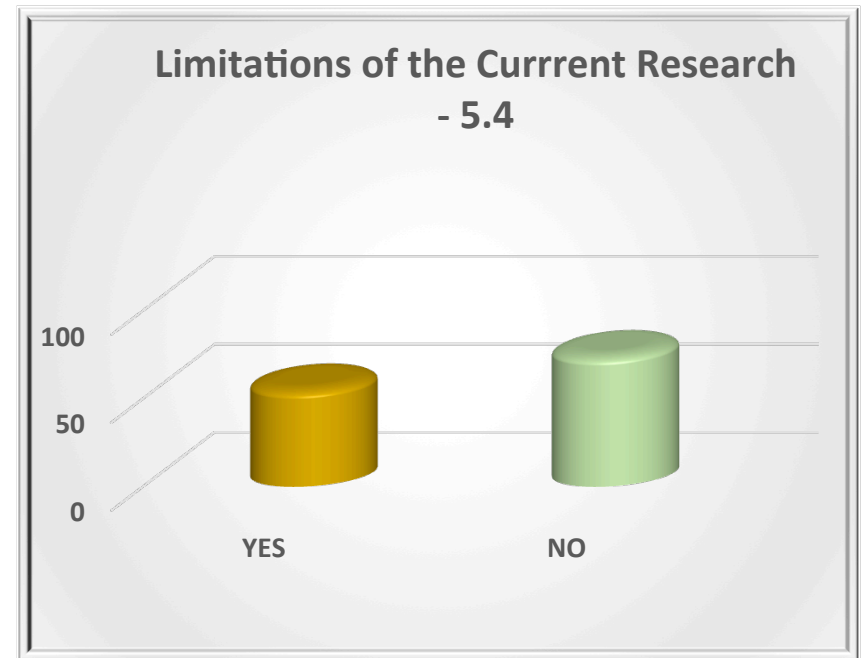
Is there an adequate description of the context in which the research was carried out?

SR on STPA : conducting

□ SYNTHESIS 5: Case study – level of evidence



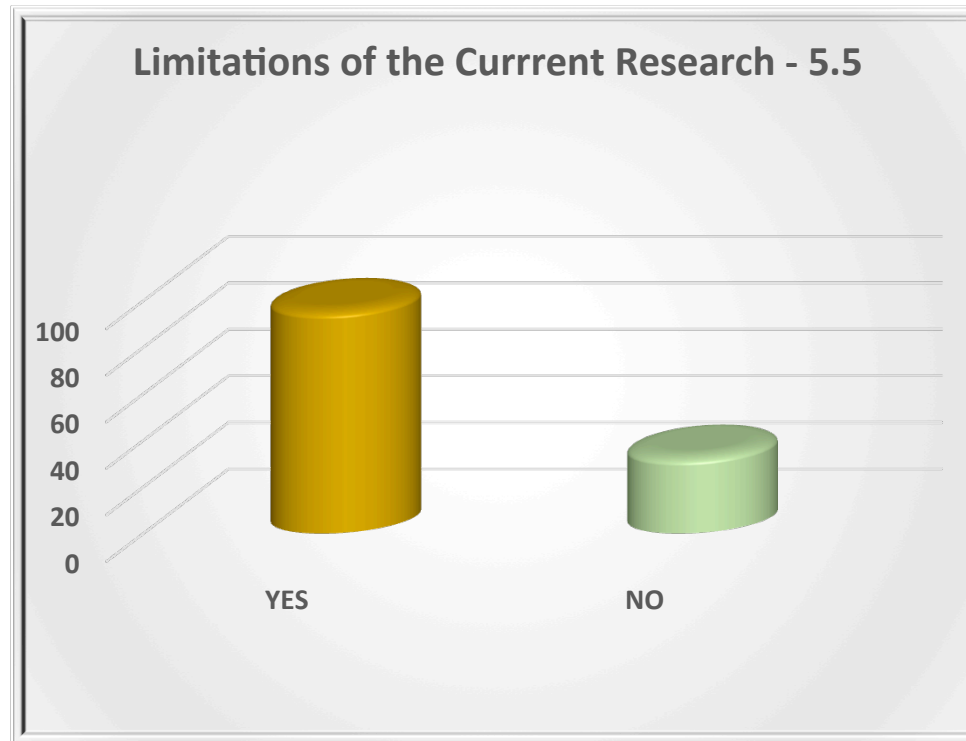
Was the data collected in a way that addressed the research issue?



Was the data analysis sufficiently rigorous?

SR on STPA : conducting

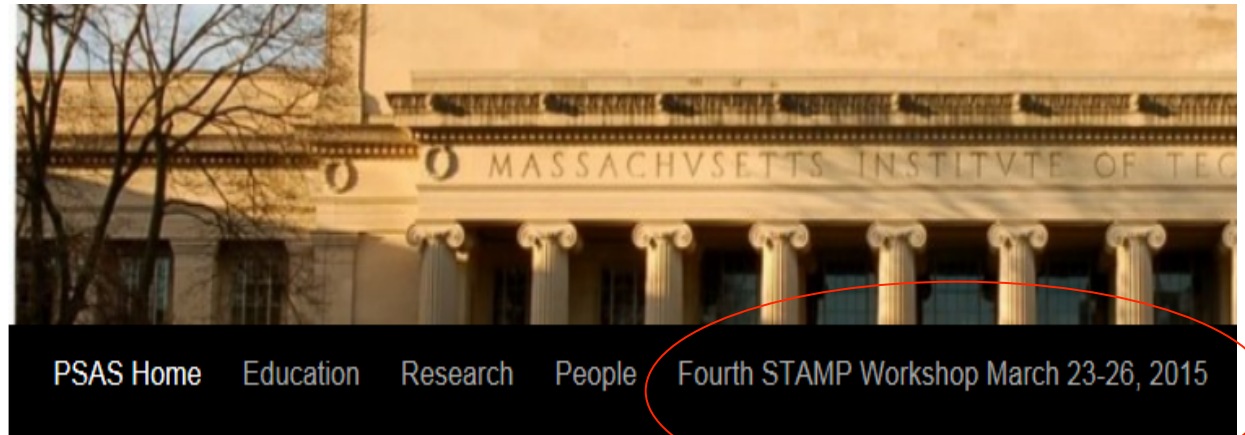
❑ SYNTHESIS 5: Case study – level of evidence



Does the researcher have experience in the case study area?

SR on STPA : reporting

REPORTING THE REVIEW: dissemination the results



Fourth STAMP Workshop at MIT 2015
this presentation!! (we are not finished yet...)

AND

Scientific Journal....(after the second phase of this Systematic Review (to submit in the second semester/2015)).



Discussion: STPA strengths

- ❑ Can be analyzed not only safety aspects, but also functional goals. [5]
- ❑ Identified more casual factors for quality losses than FMEA or FTA, including component interactions, software flaws, and omissions and external noises. [6]
- ❑ Besides to address misbehaviors due to software problems, may help address regulatory concerns. [7]



Discussion: STPA strengths

- ❑ Identify potential hazard causes in human controller by analyzing patterns of mistakes caused by cognitive behaviors errors. [8]
- ❑ STAMP framework aids in solving "old" engineering management problems: traceability, interface management, documentation of assumptions and limitations, etc. [9]
- ❑ The major benefit in our context was the support by STPA in categorizing risks and causes. [10]



Discussion: STPA opportunities

- ❑ In multiple controllers case, it is important to understand interaction (interference). [11]
- ❑ How to develop real-time constraints? [12]
- ❑ 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. [10]



Discussion: STPA opportunities

- ❑ How to filter relevant contexts to hazards to avoid unnecessary scenarios? [13]
- ❑ How to develop detailed constraints in step 2? How to develop efficient safety constraints without redundancy ? [12]
- ❑ Which domains to take into account during the analysis (software engineering and hardware engineering) By knowing the work practices of an engineering discipline one can better judge the possibility that the causes identified in step 2 of STPA will occur. [10]



Discussion: next step

Phase 2:

- ☐ Include in the SR the Workshop 2015 presentations and more articles on STAMP/STPA.
- ☐ Limiting the bias: redundant works (STPA Workshop presentations versus Conference papers versus Scientific Journal papers).
- ☐ Introducing new questions for the STAMP / STPA Systematic Review.
- ☐ Dissemination of results in the “cloud” and submitting a paper to a scientific journal.



References

- [1] 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.
- [2] Kitchenham, Dybå, Jorgensen, Evidence-based software engineering . 26th International Conference on Software Engineering (ICSE 2004), 2004, pp. 273–281.
- [3] Kitchenham, Procedures for Performing Systematic Reviews, Joint Technical Report. Software Engineering Group, Dep of Computer Science, Keele University, 2004.
- [4] Vergnes,] Marchal-Sixou, Nabet, Maret, Hamel. Ethics in systematic reviews, Journal Medical Ethics, March 2011.
- [5] Thomas, J. Extending and Automating STPA for Requirements Generation and Analysis. STAMP Workshop 2012.
- [6] Goerges. The Application of STPA in Commercial Product Development to Identify Causal Factors for Quality TM Losses. STAMP Workshop 2013.



References

- [7] Torok, Geddes. Systems Theoretic Process Analysis (STPA) Applied to a Nuclear Power Plant Control System. STAMP Workshop 2013.
- [8] Hoshino. Applying Human Mental Model to STAMP/STP. STAMP Workshop 2014.
- [9] Pelegrin. Evaluating Project Safety (System Engineering and Safety Management) in an Organization. STAMP Workshop 2013.
- [10] Asplund. Safety-Guided Design through System-Theoretic Process Analysis, Benefits and Difficulties. 30th International System Safety Conference, 2012.
- [11] Ujiie, Ishimatsu. Handling Multiple Controllers in STPA. STAMP Workshop 2012.
- [12] Yahia, Fawzy. STAMP/STPA case study Range Extender System for Electric Vehicles. STAMP Workshop 2013.
- [13] Fleming. ARP 4761 and STPA. STAMP Workshop 2014.

Systematic review on STPA:
A preliminary study

Thank you!

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

carloslahoz@gmail.com

synararosa@gmail.com

