Functional Fault Tree as Input to Hazard Analisys Using STAMP/STPA Methodology for Remote Tower (r-TWR) in Civilian and Militar Purposes

Laércio Quintanilha Fogaça Júnior
Escola Politécnica da Universidade de São Paulo
E-mail: laercio.junior.pmp@bol.com.br

João Batista Camargo Júnior
Escola Politécnica da Universidade de São Paulo
E-mail: joaocamargo@usp.br

Computer and Digital Systems Engineering Department (PCS)
School of Engineering (Escola Politécnica - Poli)
University of São Paulo (USP)
São Paulo, Brazil

Index

- **Introduction**
  - **Subject relevance;**
  - **r-TWR.**

- Conceptual Aspects
  - Architecture used in the case study;
  - Functional Fault Tree Analisys (FTTA);
  - STAMP/STPA.

- Case Study
  - Functional Fault Tree Analisys as input for STAMP/STPA.

- Conclusion

Introduction (1/1)

Subject relevance

- Increasing demand for air transport in recent years x Lack of investments in airports;
- New technologies (embedded and not embedded) optimized shipping routes and air space navigation;
- Ground components did not get the same evolution level and became the bottleneck in the aerospace system.

r-TWR (Remote Control Tower)

- An air traffic control tower whose purpose is to execute exactly the same tasks performed by traditional control towers, but in another physical location than the airport;
- Has been considered the best option to quickly increase small & medium sized airports capacity;
- Has been tested in several countries.
- What about the safety of this new system?

Index

- Introduction
  - Subject relevance;
  - r-TWR.

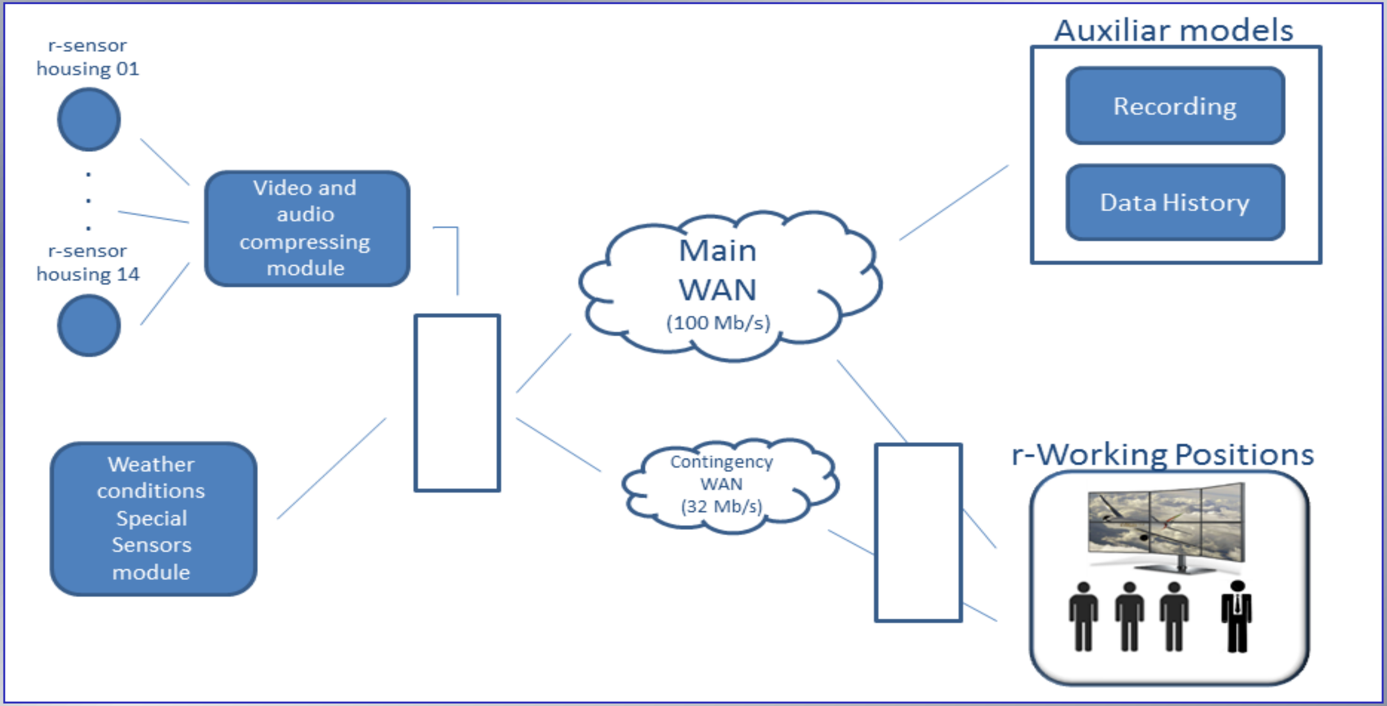
- **Conceptual Aspects**
  - **Architecture used in the case study;**
  - **Functional Fault Tree Analisys (FTTA);**
  - **STAMP/STPA.**

- Case Study
  - Functional Fault Tree Analisys as input for STAMP/STPA.

- Conclusion

Conceptual Aspects (1/1)

Architecture used in the case study



Conceptual Aspects (2/2)

Functional Fault Tree Analisys (FTTA)

- Systematic and stylized deductive process whereby an undesired event is identified and a logical diagram is constructed showing the logical event relationships;
- It was originally developed in 1961 by H. A. Watson at Bell Telephone Laboratories;
- The person/team in charge of the construction of the FFTA, know the whole system thoroughly.

STAMP/STPA

- STAMP (System-Theoretic Accident Model and Processes) is an accident causation model based on systems theory that treats accidents as a dynamic control problem;
- From the STAMP perspective, the right control actions applied at the right time, from the right control process to the right controlled process, avoid hazards and accidents;
- STPA (System-Theoretic Process Analysis) is used in STAMP to do the Hazard Analysis; it follows 4 steps: identify accidents and hazards; construct the control structure; identify unsafe control actions and finally identify causal factors and control flaws.

Index

- Introduction
  - Subject relevance;
  - r-TWR.

- Conceptual Aspects
  - Architecture used in the case study;
  - Functional Fault Tree Analisys (FTTA);
  - STAMP/STPA.

- **Case Study**
  - **Functional Fault Tree Analisys as input for STAMP/STPA.**

- Conclusion

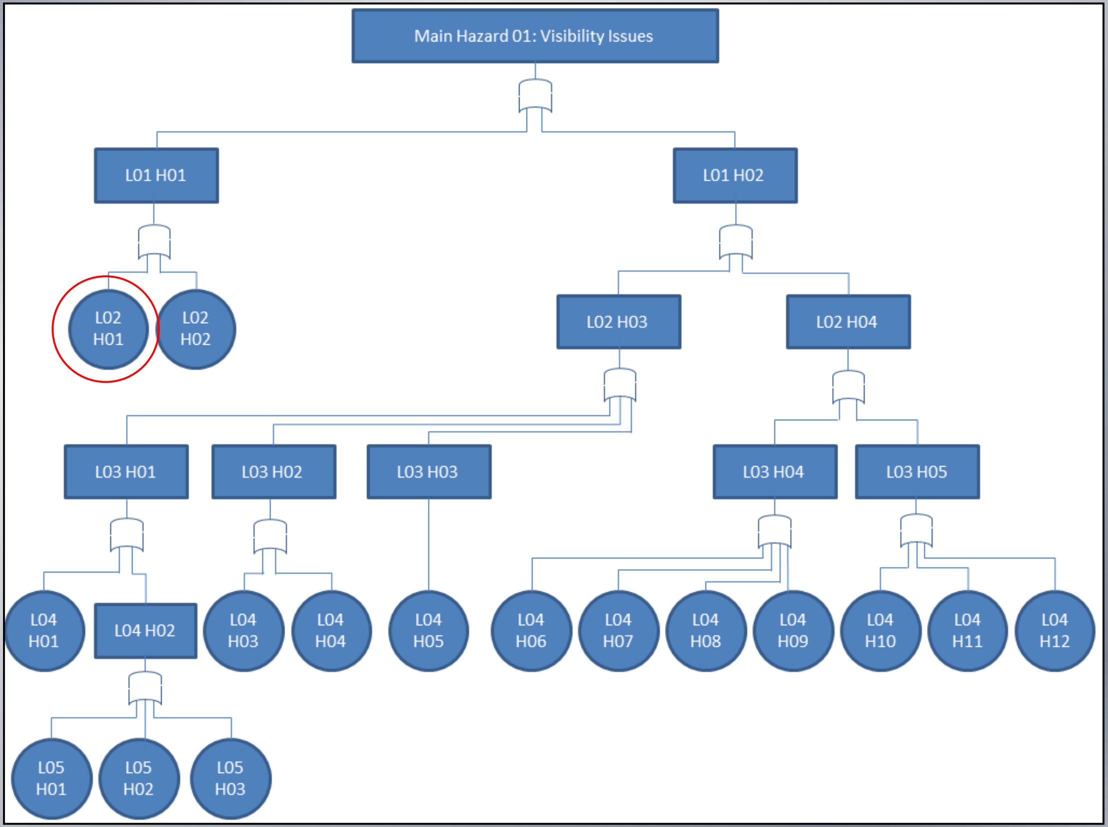
Case Study (1/3)

Functional Fault Tree Analisys as input for STAMP/STPA

- Functional Fault Tree Analisys (FFTA) will not be used to handle a fault, but a hazard.

- The purposes of using FFTA technique are to formalize the hazards and their main raisers and to make sure all potential raisers are tracked.

- Having the result of the FFTA as an input to STAMP/STPA is to complement – and do not replace – the hazards found by the specialists in the hazard analysis phase.



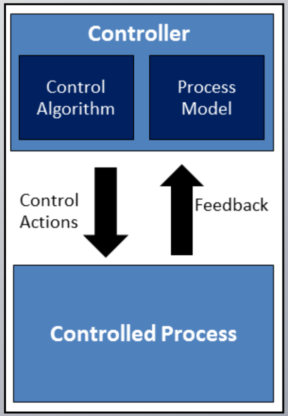
Case Study (2/3)

Functional Fault Tree Analisys as input for STAMP/STPA

- The STPA Hazard Analysis follows 4 steps: identify accidents and hazards; construct the control structure; identify unsafe control actions and finally identify causal factors and control flaws.

- Once a hazard has been identified by the specialists, the next STPA phase is to build a control structure for that hazard.

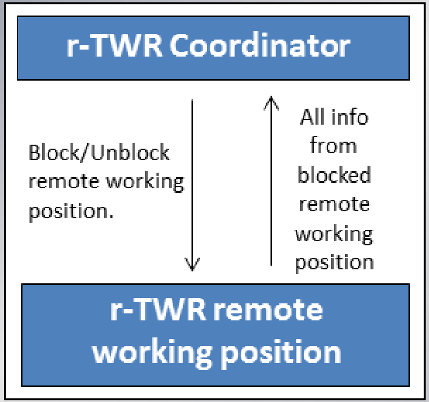
- The event handled here is the L02 H01: Intentional. Basically, the possibility of an operator intentionally taking actions that may lead to the main Hazard is treated.



Case Study (3/3)

Functional Fault Tree Analisys as input for STAMP/STPA

- Control structure designed for the condition/event L02 H01.



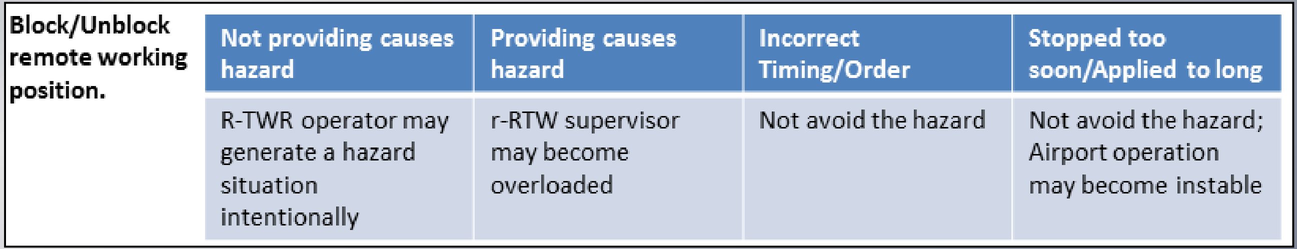
r-TWR Coordinator

Block/Unblock remote working position.

All info from blocked remote working position

r-TWR remote working position

- Unsafe control actions checking .



Block/Unblock remote working position.	Not providing causes hazard	Providing causes hazard	Incorrect Timing/Order	Stopped too soon/Applied to long
	R-TWR operator may generate a hazard situation intentionally	r-RTW supervisor may become overloaded	Not avoid the hazard	Not avoid the hazard; Airport operation may become instable

Index

- Introduction
  - Subject relevance;
  - r-TWR.

- Conceptual Aspects
  - Architecture used in the case study;
  - Functional Fault Tree Analisys (FTTA);
  - STAMP/STPA.

- Case Study
  - Functional Fault Tree Analisys as input for STAMP/STPA.

- **Conclusion**

Conclusion (1/1)

Applying this approach we found:

- Formalize and document which aspects were considered for a particular hazard when starting the control process construction.

- Due this documentation, new people in the project can fully understand what was done and quickly start contributing with the project team.

- Changes are a constant in a project. Having this documentation is a great asset when needing to handle with changes.

Dziekujemy

KIITOS Vielen Dank

Terima kasih

Täname teid Gracias Grazie

Thank You

Dankie

Paldies Tak Obrigado

Merci DÈKOJAME

DEKUJEME VÁM Bedankt

Köszönjük

Laércio Quintanilha Fogaça Júnior
E-mail: laercio.junior.pmp@bol.com.br

João Batista Camargo Júnior
E-mail: joaocamargo@usp.br