FUNCTIONAL FAULT TREES 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
Rua Alberto Hodge, n 220 – Tel.: 2691-8036 – E-mail: laercio.junior.pmp@bol.com.br

João Batista Camargo Júnior
Escola Politécnica da Universidade de São Paulo
Av.: Professor Luciano Gualberto, Trav. 3, n 158 – Tel.: 3091-5401 – E-mail: joaocamargo@usp.br

ABSTRACT

STAMP and STPA have been increasingly used in qualitative and quantitative risk and hazard assessments in several areas of the airspace industry. The main goal is to present the use of functional fault trees as an input to the hazard analysis using the STAMP and STPA methodology, working as a formal way to record what was considered when creating the control structure and a complement to the survey with specialists. The article provides one example of this use in air traffic remote tower (r-TWR) project where the architecture used is based on a real r-TWR implementation.

.

Keywords: Remote Control Tower, r-TWR, STAMP, STPA, Hazard Analysis.

1. INTRODUCTION

With the high and increasing demand for air transport in recent years, countries all over the world began to face the need of increasing the efficiency of their existing airspace systems.

In the air, new technologies (embedded and not embedded), optimized shipping routes and air space navigation techniques, made air travel time smaller, decreased the required spacing between aircrafts and optimized fuel consumption – without compromising the airspace system or aircraft safety.

These two factors combined - growing demand and optimized aeronautical routes utilization - significantly increased the pressure on airports and airfields - ground components and their controls - since the latter did not follow the same evolution curve observed in the air components.

Several solutions have been discussed and proposed to enhance and to optimize the capacity of airports and airfields, one of which has gained great attention and notoriety: the use of Remote Control Towers (r-TWR).

1.1. REMOTE TOWERS (r-TWRs)

A Remote Control Tower (r-TWR) is an air traffic control tower whose purpose is to execute exactly the same tasks performed by traditional control towers (TWR), but differing that the former is not physically in the aerodrome or controlled airport, but in another physical location.

"With lower construction and operating costs, standardized-trained staff, greater easiness to investigate accidents or incidents and less time to be operational than TWR" (SAAB, 2015), the r-TWR has proved not only a very viable option - already being tested and implemented in countries such as Sweden, Norway, USA and Australia - but "as a survival measure for small and medium-sized airports, due to their operating costs" (SAAB, 2015).

Given the importance r-TWRs have achieved in recent years, and the growth of risk and hazard analysis methodologies, complex systems-oriented, our main goal is to demonstrate the use of Functional Fault Tree as an input for the qualitative hazard analysis in his new technology (r-TWR) using the complex system orientated STAMP / STPA methodology.

2. CONCEPTUAL ASPECTS

2.1. ASSUMPTIONS & DEFINITIONS

Since risk assessment and hazard analysis are totally dependent on the system and on its architecture, before starting any analysis, it was necessary to define a basic architecture for using the r-TWR.

Given the lack of full technical information on the architectures tested and architectures implemented in real r-TWR projects, the number of possible variations of architecture due to the final purpose (civilian/military) and the specific needs of an airport/airfield in particular, the components used in an implementation conducted by a Swedish company in a r-TWR project for a civilian use on Alice Springs airport in Australia were researched. Based on this architecture, a type of architecture was created that formed the basis for the hazard analyses presented herein.

This airport/r-TWR project was chosen due its characteristics - midsized regional airport according to the classification used by ANAC (ANAC, 2015), with two lanes (the largest can accommodate a Boeing 747) - as well as the complexity of the project itself (r-TWR is physically in Adelaide, 1500 km far from the airport in Alice Springs).

Figure 1: Alice Springs Airport (adapted from www.airforce.gov.au)

The macro components used in the basic architecture considered in this article are presented as follows:

- 03 air traffic controllers: air traffic controllers are responsible for giving all the instructions to the aircraft within its jurisdiction and report any anomalies within their remote working position. They work as a guide to all approaching/landing and taking off procedures, which are important to the success and the safety of the whole system.

- 01 air traffic controller supervisor: the supervisor is responsible for balancing the workload between controllers and ensures that procedures are being properly executed.

- 14 remote sensor housing, each of which is composed of 01 high-definition camera, 01 infrared thermal camera, 01 signal light gun and 01 acoustic sensor. The remote sensor housing (RSH) are the main data acquisition points for r -TWR. The redundancy of high definition and infrared cameras, not only provides distinct features but ensures that in an eventual failure of a camera, it is automatically covered by another. This ensures by design all the basic operations that depend on the data acquired by that RSH and avoid any jeopardies to the controller. Besides, the lack of specific features during an eventual camera failure - in addition to the defective camera control itself - ensures situational awareness for the team of r-TWR regarding the equipment failure.

- 01 video and audio compressing module: receives and compresses all the information generated by RSH, increasing the speed and optimizing the data transfer over the WAN; must have a fault detection component that detects any issues in the compressing module and starts to send only partial, non-compressed, information to the current working WAN.

- 01 video decompressing module: its function is decompressing the compressed data received through the WAN. It must be able to check whether the data received is compressed.

- 01 Main WAN: a dedicated wide area network to be the main way of transferring data from the airport to the r-TWR. This WAN capacity must be of about 100 Mb/s. In case of fault or malfunctioning, the data flow will be switched to the contingency WAN.

- 01 Contingency WAN: dedicated wide area network with transfer rate of about 32 Mb/s. The contingency WAN will be used only in case of fault or malfunctioning of the main WAN, since using this contingency WAN means that not all data collected from the RSH will be sent to the r-TWR.

- 01 WAN fault detection and switching module: this module must be able to validate the right operation of the wide area network and make switches between them as necessary. When the primary WAN is good to go, it must be the means of communication. If the main WAN goes off line or starts to face any operational issue that may affect its integrity, the contingency WAN must be triggered and be the main communication channel between the airport and the r-TWR. In this case, the main WAN should be constantly monitored until it is ready to restart the connection, becoming operational again. At this point, the module must switch the communication channel between the aerodrome and the r- TWR from the Contingency WAN to the Main WAN

- 04 Integrated Remote Working Positions: considers the same work position number used in the original r-TWR project design taken as basis, of 04 positions, 03 of which are operators and 01 supervisor.

- 01 data and images recording module: this module is responsible for storing all the data received by the r-TWR. The future use of such data could be training, verifying the procedures adopted by operators and by the supervisor, and investigations on incidents or accidents that may occur.

- 01 High volume data storage module: stores large the large number of data generated by the RSH, which is going to be the history of that airport operation by the r-TWR.

The architecture used as basis can be seen in Figure 2 below

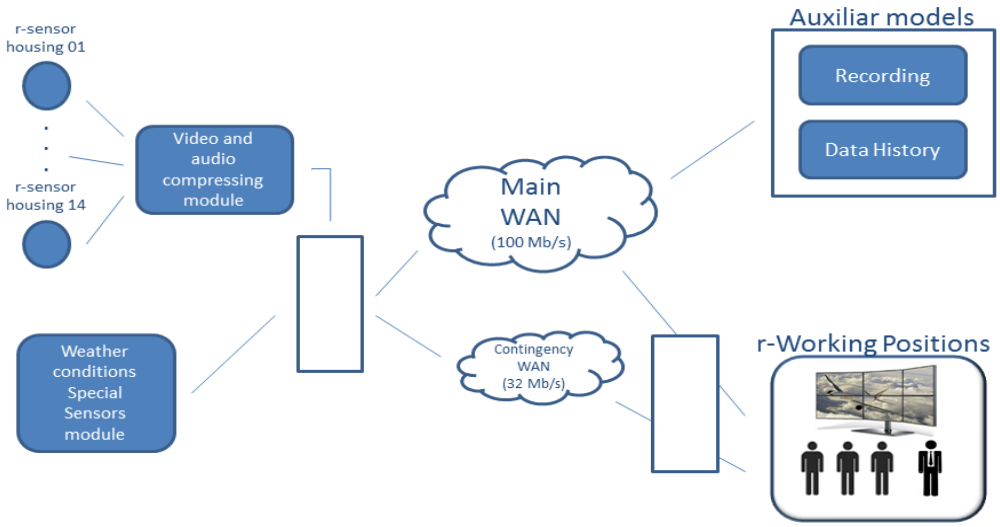

Figure 2: Architecture used in the analysis (adapted from Frequentis - 2013)

2.2. FUNCTIONAL FAULT TREE

Functional Fault Tree Analysis (FTTA) is a "systematic and stylized deductive process whereby an undesired event is identified and a logical diagram is constructed showing the logical event relationships". (NASA, 2015)

FFTA is widely used in the aerospace, electronics and nuclear industries. "It was originally developed in 1961 by H. A. Watson at Bell Telephone Laboratories to evaluate the Minuteman Launch Control System for an unauthorized (inadvertent) missile launch". (LEVESON, Nancy – 1995).

The person/team in charge of the construction of the FFTA, know the whole system thoroughly. "Every possible cause and effect of each failure condition should be investigated and related to the top even". (KECECIOGLU, Dimitri – 2002)

3. CASE STUDY

In this article context, the FFTA will not be used to handle a fault, but a hazard. The same logic applies to the levels below, since we work with events/ conditions/ situations/ controls that may generate a hazard instead of a fault.

However, the whole technique application is still the same as for a traditional functional fault tree analysis.

The purposes of using this FFTA technique are to formalize the hazards and their main raisers and to make sure all potential raisers are tracked. In this sense, it is right to statement that the goals for having the result of the FFTA as an input to STAMP/STPA method are to complement – and do not replace – the hazards found by the specialists in the hazard analysis phase.

Due the complexity and final size of this kind of analysis in the r-TWR context, we here present a single FFTA, which means a single hazard situation will be analyzed. It is worth highlighting that the method/mechanism will be exactly the same if we have 10 or 1000 hazards to be evaluated.

Figure 3 depicts the FTTA created for the hazard that is going to be used in this article, Visibility Issues. The details of the event description and its possible causes are in Table 1.

Table 1: FTTA event description details for the main hazard 01: Visibility Issues

Event	*Description*
L01H01	Human factor
L01H02	Equipment factor
L02H01	Intentional (by Operator)
L02H02	Operator´s visual deficiency
L02H03	Off site
L02H04	On site

L03H01	Low quality captured image
L03H02	Issued or delayed in image transmission
L03H03	Non expected/inappropriate captured image
L03H04	Non-operant monitor
L03H05	Low quality image monitor
L04H01	Extreme weather conditions
L04H02	Camera
L04H03	Main WAN datalink
L04H04	Link between housing and video/audio compressing module
L04H05	Housing camera position
L04H06	Failure in the monitor cable

L04H07	Crashed monitor
L04H08	Energy blackout
L04H09	Off line monitor
L04H10	Failure in the monitor cable connection
L04H11	Monitor set up
L04H12	Intermittent off line monitor
L05H01	Housing camera set up
L05H02	Housing camera is off line
L05H03	Housing camera is unable to generate the images due to external conditions

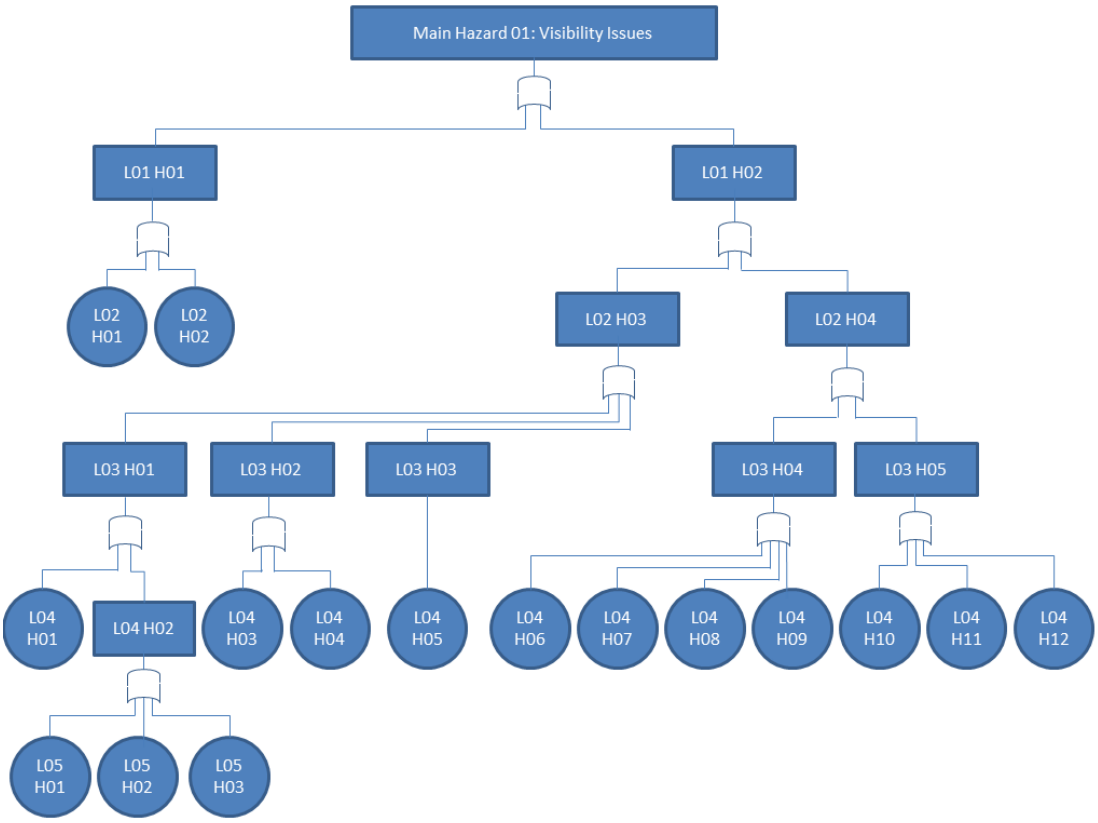

Figure 2: FFTA used for the main hazard handled in this article

3.1. USING THE FUNCTIONAL FAULT TREE AS AN INPUT TO STAMP/STPA ANALISYS

The STAMP (System-Theoretic Accident Model and Processes) is an accident causation model based on systems theory that treats accidents as a dynamic control problem (vs. a failure problem). It includes the entire socio-technical system, component interaction accidents, software and system design errors and human errors. (LEVESON, Nancy; THOMAS, John – 2012)

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. The concept above is demonstrated in Figure 4.

Due this statement, it is possible to conclude that, from the STAMP perspective,

hazards and accidents are caused basically by inadequate or inappropriate control.

In order to find inadequate and inappropriate controls in design, the STPA (System-Theoretic Process Analysis) Hazard Analysis was created.

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.

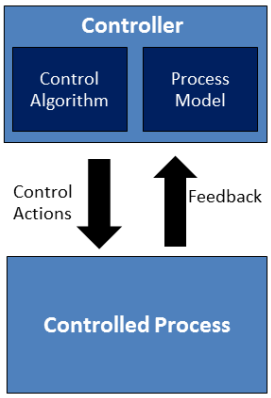

Figure 4: Role of Process Models in Control (Leveson, 2011)

Once the hazard has been identified by the specialists, the next STPA phase is to build a control structure for that hazard. In order to create the most effective control, it is mandatory to understand all the events and conditions that may lead to that hazard.

The FFTA provides better understanding and formalization regarding which events and conditions have been considered when handling with that hazard and the construction control related to it.

Having this input, other specialists can quickly understand what was considered when the control structure was built and to more easily evaluate if all the events and conditions were considered. Besides, if changes in the system are necessary, reviewing all hazards and their control structures will be quicker, since all the events and conditions considered for that Hazard are documented in the FTTA.

For purposes of this article, a single event/condition leading to a hazard situation was analyzed: an intentional behavior from a traffic control operator in r-TWR that may lead to the hazard.

Note that, all the other conditions and events that may lead to this hazard (visibility issues) must be analyzed and their control structure must be implemented in order to have the final control structure for hazard visibility issues.

The next section details the analysis for the event/condition L02 H01: Intentional.

3.2 CREATING THE CONTROL STRUCTURE IN STPA

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.

The control structure suggested for this event is allowing the r-TWR coordinator to assume the functions from an operator, taking control over its remote working position in r-TWR.

For allowing that, the systems design must provide the functionality in which the r-TWR coordinator can block/unblock other remote working positions, taking all their information and controls to his/her own remote working position.

With this control structure in place (see figure 5) and following the next steps in STPA for this analysis, it is possible to check which issues or hazards this control structure may cause.

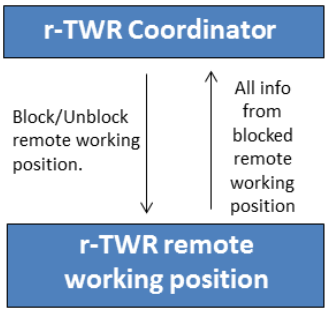

Figure 5: Control structure designed for the condition/event L02 H01

After this control structure has been analyzed, a table must be filled in order to move forward. In table 2, it is possible to see all the information that must be provided and which consequences and details need to be considered to provide this functionality/structure control.

Table 2: Unsafe control actions checking (adapted from Phd. John Thomas, 2013)

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

4. CONCLUSIONS

The use of FTTA as an input for the STAMP and STPA methodologies proved to be a great asset when applied to the real case that was the subject of this article.

The first positive point in this approach is the formalization and documentation, in which aspects are considered for a particular hazard when starting the control process construction. The high volume of hazards that needs to be analyzed in a complex system such as an r-TWR system and the complexity that control processes can present require a simple and comprehensive previous documentation which is fully achieved with the implementation of FTTA as input for the STAMP and STPA.

The second positive point in this approach is that due to the constant changes undergone by control processes– such changes are natural, expected and necessary for proper system design -, the documentation of what was considered when creating the control processes to handle each hazard helps track what has been changed, how and why.

A third positive finding is related to another project characteristic. Since there is always the chance of replacing or adding new people during the system design phase. The documentation of all the considerations used for each hazard, provided by the FTTA, allows new people in the team to contribute faster to the project, or even raise points which, according to the FTTA documentation have not been considered.

5. REFERENCES

KECECIOGLU, Dimitri. Reliability engineering handbook Volume 2 – 2002

LEVESON, Nancy. Safeware System Safety and computers – 1995

LEVESON, Nancy; THOMAS, John. Engineering a safer world – 2012

CHECKLAND, Peter – Systems Thinking Systems Practice – 1981

NASA, National Aeronautics and Space Administration, available at: http://www.hq.nasa.gov/office/codeq/risk/docs/ftacourse.pdf. Accessed on Aug-25-2015.

RAAF, Royal Australian Air Force, available at: www.airforce.gov.au. Accessed on Aug-25-2015.

SAAB, available at: http://saab.com/security/air-traffic-management/air-traffic-management/remote-tower/ Accessed on Aug-25-2015.

FREQUENTIS, available at: http://www.frequentis.com/en/us/solutions-portfolio/air-traffic-management/#! Accessed on Aug-25-2015.

ANAC, Civilian national aviation agency, available at: http://www2.anac.gov.br/arquivos/pdf/horaPicoForWeb.pdf. Accessed on Aug-25-2015.